

# **GUESTGATE™ MK II**

## **Wireless 300N Hotspot Gateway**

### **HANDBUCH**

MODELL 524827



INT-524827-UM-0810-01

## Sicherheits- und Rechtshinweise



Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte bieten angemessenen Schutz vor schädlichen Störungen beim Betrieb des Geräts in Gewerbegebieten.

Beim Betrieb dieses Geräts in Wohngebieten sind Interferenzen wahrscheinlich. In diesem



Fall muss der Nutzer die Interferenzen auf eigene Kosten beseitigen. Dieses digitale Gerät erfüllt die Anforderungen zu Strahlenausstoß gemäß Grenzwert B EN55022/1998 und die Anforderungen zu Störfestigkeitseigenschaften gemäß EN55024/1998 in Wohn-, Gewerbe, und Leichtindustrialgebieten.

### R&TTE-Konformitätserklärung



Diese Anlage entspricht allen Anforderungen der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 09. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität (R&TTE).

Die R&TTE-Richtlinie ersetzt seit dem 08. April 2000 die Richtlinie 98/13/EEC und hebt diese auf.

### Elektro- & Elektronik-Altgeräte

#### Entsorgung von Elektro- und Elektronik-Geräten

**(Anwendbar in der Europäischen Union und anderen europäischen Ländern mit getrennten Sammelsystemen)**



Dieses Symbol auf dem Produkt oder der Verpackung bedeutet, dass das Produkt nicht als Hausmüll zu behandeln ist. Stattdessen sollte es zu einer geeigneten Rücknahmestelle zum Recycling von Elektro- und Elektronik-Geräten gebracht werden. Durch die Sicherstellung der ordnungsgemäßen Entsorgung, tragen Sie dazu bei, negative Einflüsse auf Umwelt und Gesundheit zu vermeiden. Wenn Ihr Gerät einfach zu entfernende Batterien oder Akkus enthält, entsorgen Sie diese separat entsprechend der lokalen Bestimmungen Ihres Wohnorts. Das Materialrecycling trägt zur Bewahrung natürlicher Rohstoffe bei. Für weitere Informationen über das Recycling dieses Produkts wenden Sie sich an das zuständige Amt Ihrer Stadt, Ihren lokalen Abfallbeseitigungsdienst oder den Händler, bei dem Sie dieses Produkt erworben haben. Für Länder außerhalb der EU: Möchten Sie dieses Produkt entsorgen, wenden Sie sich an Ihre lokalen Behörden und erkundigen Sie sich über die ordnungsgemäße Art der Entsorgung.

# INHALTSVERZEICHNIS

<b>Sicherheits- und Rechtshinweise.....</b>	<b>2</b>
<b>INHALTSVERZEICHNIS .....</b>	<b>3</b>
<b>EINLEITUNG .....</b>	<b>4</b>
<i>Funktionsbeschreibung .....</i>	<i>4</i>
<i>Installationsbeispiele.....</i>	<i>6</i>
<i>GuestGate Basisfunktionen .....</i>	<i>8</i>
<b>INSTALLATION .....</b>	<b>9</b>
<i>Empfohlene Einrichtung.....</i>	<i>9</i>
<i>Erweiterte Einrichtung.....</i>	<i>14</i>
<b>EINSTELLUNGSOPTIONEN .....</b>	<b>19</b>
<i>Statusseite.....</i>	<i>19</i>
<i>Gast-Konfigurationsseite.....</i>	<i>20</i>
<i>Gastgeber-Konfigurationsseite.....</i>	<i>24</i>
<i>Konfiguration der Willkommenseite .....</i>	<i>28</i>
<i>Zeit /Planer-Konfiguration.....</i>	<i>30</i>
<i>Geräte-Einstellungen.....</i>	<i>32</i>
<i>Firmware aktualisieren .....</i>	<i>35</i>
<i>Exit-Bildschirm.....</i>	<i>37</i>
<b>FRAGEN &amp; ANTWORTEN .....</b>	<b>38</b>
<b>ANHANG.....</b>	<b>42</b>
<b>GARANTIEINFORMATIONEN .....</b>	<b>43</b>

## **EINLEITUNG**

Herzlichen Glückwunsch zum Kauf des INTELLINET NETWORK SOLUTIONS GuestGate™ MK II Hotspot Gateways. GuestGate verbindet Gäste mit Ihrem Netzwerk und beschränkt den Zugriff dabei auf das Internet (z. B. Web, E-Mail, Chat und ähnliche Anwendungen). So schützt GuestGate Ihr vorhandenes Netzwerk vor unbefugtem Zugriff durch angeschlossene Gastcomputer und schirmt diese, falls gewünscht, sogar untereinander ab. Außerdem unterstützt GuestGate erweiterte IP PnP (Plug and Play)-Technologie: Es passt sich automatisch an die TCP/IP-Einstellungen des Gastcomputers an und macht zeitaufwändiges Neukonfigurieren der Gastcomputer überflüssig. Die Mark-II-Edition unterstützt 300 Mbit/s Wireless N, Radius-Authentifizierung und erweiterte Logging (Aufzeichnungs-)Optionen.

GuestGate integriert sich nahtlos in Ihr vorhandenes Netzwerk, eine weitere Konfiguration des GuestGates ist nur in den seltensten Fällen notwendig. GuestGate bietet alle Kernfunktionen schlüsselfertig für den schnellen Einsatz.

## ***Funktionsbeschreibung***

### **Internetzugang für Gäste**

GuestGate wurde hauptsächlich entwickelt, um Ihren Gästen einen einfachen Internetzugang ohne zusätzliche Konfiguration zur Verfügung zu stellen. GuestGate nutzt den bestehenden Internetzugang Ihres Netzwerks, um Internet- und E-Mail-Zugriff für Gäste in Konferenzräumen, Hotels oder öffentlichen Plätzen mit WLAN-Anbindung zur Verfügung zu stellen. Darüber hinaus schützt GuestGate sicherheitsrelevante Bereiche des bestehenden Netzwerks, indem es den Zugriff durch angeschlossene Gastcomputer verweigert. Kurz: Gäste haben Zugriff auf das Internet, aber Ihr eigenes Netzwerk, d. h. Ihre Datei-, E-Mail- oder Anwendungsserver bleiben geschützt.

### **Passwortgeschützter Internetzugang für Gäste**

Ihr Netzwerkadministrator kann für den Internetzugang ein Passwort festsetzen. Dies ist eine wichtige Funktion, wenn Sie Gebühren für den Internetzugang erheben möchten oder um zu verhindern, dass sich Unbefugte über einen am GuestGate angeschlossenen, ungeschützten WLAN Access Point anmelden und Ihre Bandbreite nutzen.

### **Individuelle Startseite für Ihre Gäste**

Sie können die Startseite innerhalb weniger Sekunden ändern. Passen Sie Text und Format an, laden Sie Ihr eigenes Logo hoch oder ändern Sie den gesamten HTML-Code. Die Startseite wird angezeigt, wenn ein Gast sich zum ersten Mal mit dem Internet verbindet. Diese „Willkommenseite“ kann beispielsweise genutzt werden, damit Gäste Ihren allgemeinen Geschäftsbedingungen zustimmen, falls gewünscht kann sie auch vollständig deaktiviert werden.

### **IP PnP**

In vielen Situationen ist es notwendig, dass der Netzwerkadministrator die TCP/IP-Einstellungen eines Gastcomputers ändert, weil diese nicht mit den vorhandenen Netzwerkeinstellungen kompatibel sind oder weitere Einstellungen erforderlich sind.

GuestGate beseitigt diesen Schritt vollständig, indem es sich automatisch an die TCP/IP Einstellungen des Gastcomputers anpasst.

### **Bandbreitenbegrenzung**

GuestGate lässt Sie festlegen, welcher Anteil Ihrer Internetbandbreite dem Gastnetzwerk zur Verfügung gestellt werden soll. Upload- und Download-Bandbreite können individuell konfiguriert werden.

### **Layer 3 Client Isolation Funktion**

An öffentlichen Plätzen mit einem frei zugänglichen Wireless Access Point ist man oftmals um die Sicherheit besorgt. GuestGate schützt nicht nur Ihr Gastgebernnetzwerk vor unbefugten Zugriffen durch Gastcomputer, sondern geht noch einen Schritt weiter. Wenn die Option „separates Netzwerk für jeden Benutzer“ aktiviert ist, hat kein Gastcomputer Zugriff auf einen anderen Gastcomputer. In diesem Modus teilt GuestGate jedem Gastcomputer ein eigenes, zufällig generiertes Netzwerk zu. Diese Option ist standardmäßig aktiviert.

### **Paketfilter**

Blockiert den Zugriff auf bestimmte Webseiten oder ganze IP-Adressbereiche.

### **300 Mbit/s Wireless N Unterstützung**

GuestGate MK II verfügt über integrierte Wireless-LAN-Unterstützung für Übertragungsgeschwindigkeiten bis zu 300 Mbit/s. Neben der neuesten Wireless-N-Technologie werden auch die älteren Wireless-G- und Wireless-B-Standards unterstützt.

### **4 Port 10/100 Auto Sensing LAN Switch**

GuestGate bietet vier 10/100 Mbit/s LAN Switch Ports für den Anschluss von PCs, Notebooks, anderer Switches oder Wireless Access Points.

### **Webbasiertes Administrator-Interface**

Die Konfiguration ist komplett Webbrowser-gestützt. Aus Sicherheitsgründen kann das Administratormenü nur aus dem Host (Gastgeber)-Netzwerk aufgerufen werden.

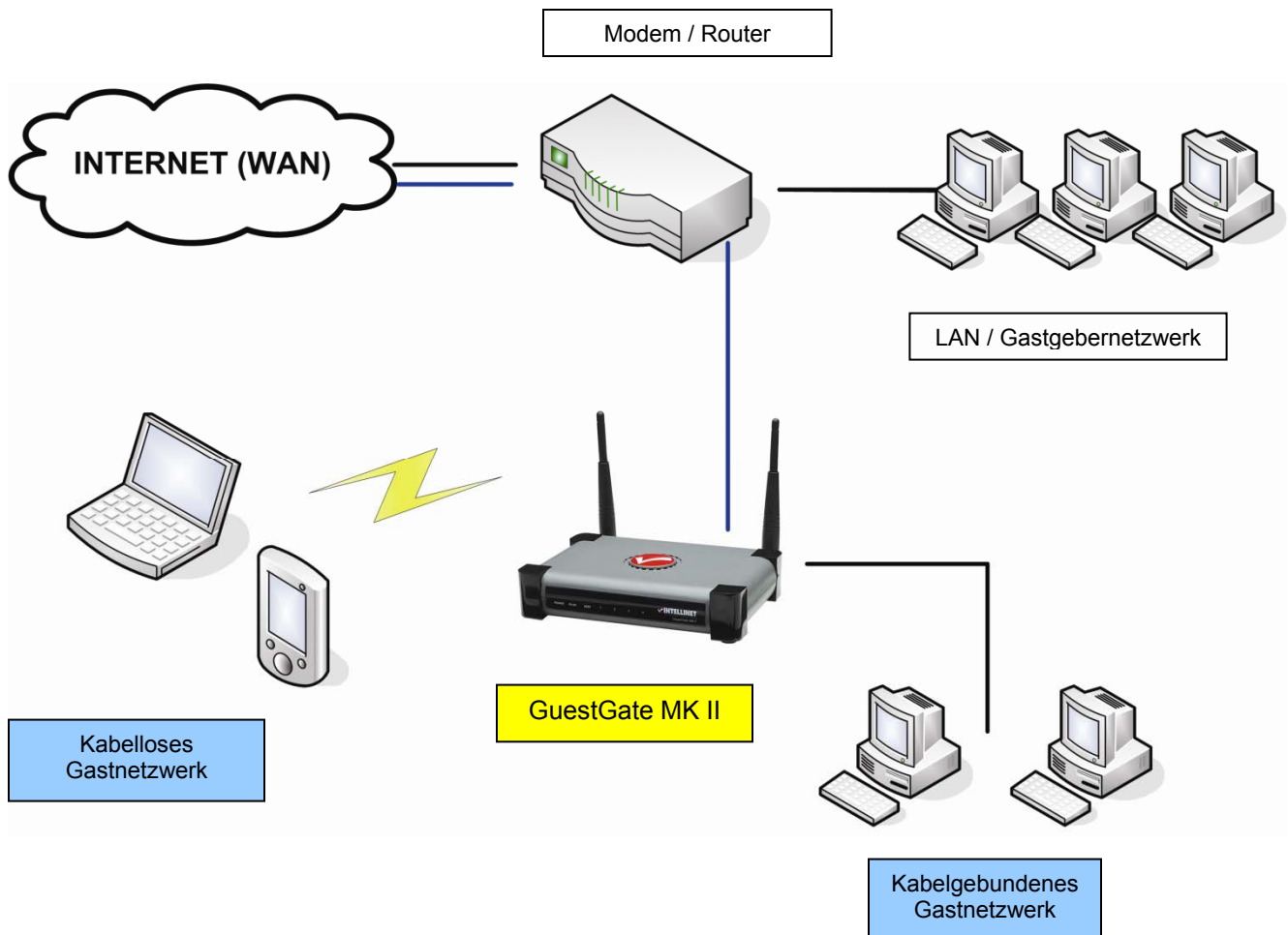
### **Firmware-Aktualisierungen über den Webbrowser**

Aktualisieren Sie die GuestGate-Firmware bequem und einfach über den Webbrowser Ihrer Wahl.

## Installationsbeispiele

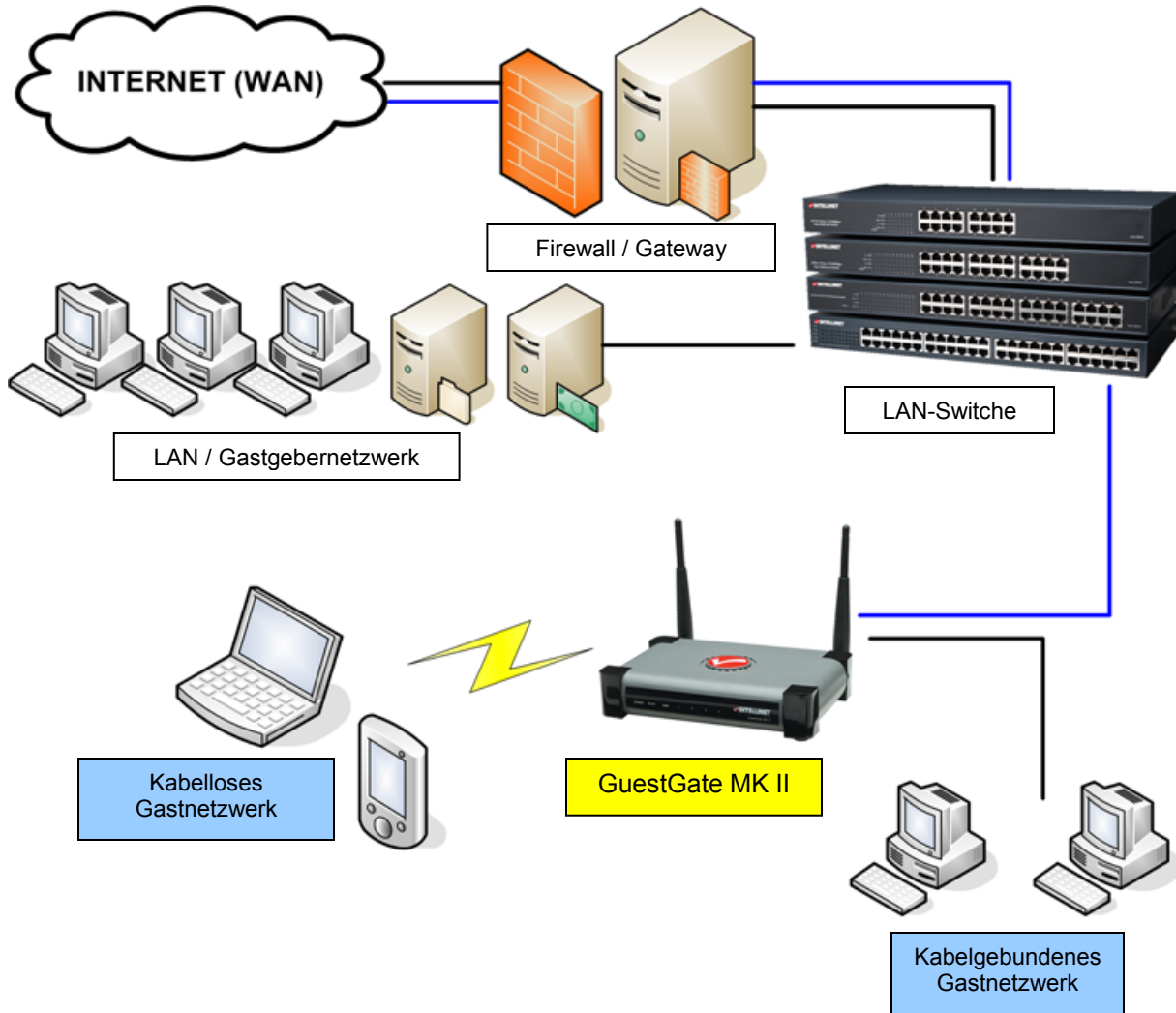
### GuestGate in einer SOHO-Netzwerk-Umgebung (Kleinunternehmen und Homeoffice)

Eine typische Netzwerkumgebung, in der der Internetzugang durch einen NAT-Router mit integrierter Firewall zur Verfügung gestellt wird.



## GuestGate in einer SMB-Umgebung (kleine und mittlere Unternehmen)

In größeren Netzwerken wird GuestGate mit einem beliebigen Switch verbunden, der sich hinter der/dem Firewall/Gateway/Router befindet.



## ***GuestGate Basisfunktionen***

### **Ports**

GuestGate verfügt insgesamt über fünf 10/100 RJ-45 Ports. Über einen Port wird GuestGate mit dem Gastgeber-Netzwerk verbunden (Host Port), vier weitere Ports stehen zum Anschluss für Gastcomputer zur Verfügung (Guest Ports). An die Guest Ports können Hubs, Switches, Wireless Access Points, PCs oder Notebooks angeschlossen werden.

### **Host (Gastgeber-) Port**

Üblicherweise erhält GuestGate eine IP-Adresse von einem DHCP-Server, der sich bereits im vorhandenen Netzwerk befindet. GuestGate analysiert das Netzwerk und erhält alle Informationen, die für den Internetzugang notwendig sind. Das DHCP-Server-Log zeigt die HOST-IP-Adresse des GuestGates. Für den Fall, dass kein DHCP-Server vorhanden ist, wird die IP-Adresse des GuestGates auf den Standard 192.168.2.1 gesetzt. In diesem Fall ist eine manuelle Konfiguration der HOST-IP-Einstellungen erforderlich.

### **Guest (Gast-)Ports**

GuestGate vergibt IP-Adressen an die angeschlossenen Gastcomputer. IP PnP Technologie macht weitere Konfigurationen der Gastcomputer überflüssig. Der standardmäßige DHCP-IP- Adressbereich lautet 172.16.xxx.xxx. Das Ändern der Gäste-IP-Einstellungen ist über das Administrator-Webinterface möglich.

### **Guest Ports mit Layer 3 Client Isolation aktiviert**

Ist die Layer 3 Client Isolation aktiviert, weist GuestGate jedem verbundenen Gastcomputer ein anderes IP-Netzwerk (Subnetz) zu. Da diese Zuweisung nach dem Zufallsprinzip erfolgt, ist es für Hacker nahezu unmöglich, die IP-Einstellungen des anderen Gastcomputers zu ermitteln und Zugriff zu erlangen. Diese Einstellung ist standardmäßig aktiviert. Sie kann auf der Gastkonfigurationsseite der Administrator-Weboberfläche deaktiviert werden. Die Option lautet „separates Netzwerk für jeden Benutzer“.

### **Zeit / Planer**

Sie können einen Zeitraum einstellen, in dem GuestGate Internetzugang erlaubt. Mögliche Werte sind entweder immer Online oder auf einem Plan basierend (Woche, Tag und Zeit).

### **Zugriff auf das Administrator-Webinterface**

Die gesamte Konfiguration des GuestGates ist webbasiert, jeder Standard-Webbrowser wird unterstützt. Aus Sicherheitsgründen kann das Administratormenü nur über den Host-Port aufgerufen werden. GuestGate weist alle Zugriffsversuche durch die Gast-Ports ab.

### **Internetzugang für Gäste und Startseite**

Wenn ein Gastcomputer zum ersten Mal versucht auf das Internet zuzugreifen, wird eine „Willkommenseite“ im Webbrowser angezeigt. Diese Startseite kann im Administratormenü konfiguriert und modifiziert werden. Gäste müssen Ihren Allgemeinen Geschäftsbedingungen zustimmen, um Internetzugang zu erhalten. Falls die Option Gastpasswort aktiviert ist, muss zunächst ein Passwort eingegeben werden. Diese Autorisation wird nur einmal benötigt. GuestGate speichert alle autorisierten Gastcomputer, bis GuestGate neu gestartet wird. Nach einem Neustart von GuestGate sehen auch bereits autorisierte Gäste die Startseite erneut. Wenn ein Gastcomputer mehr als 10 Minuten von GuestGate getrennt ist, wird die Startseite ebenfalls erneut geladen.



# INSTALLATION

## **Empfohlene Einrichtung**

Diese Einrichtungsmethode setzt voraus, dass sich ein DHCP-Server, z. B. ein Router, in Ihrem Netzwerk befindet.

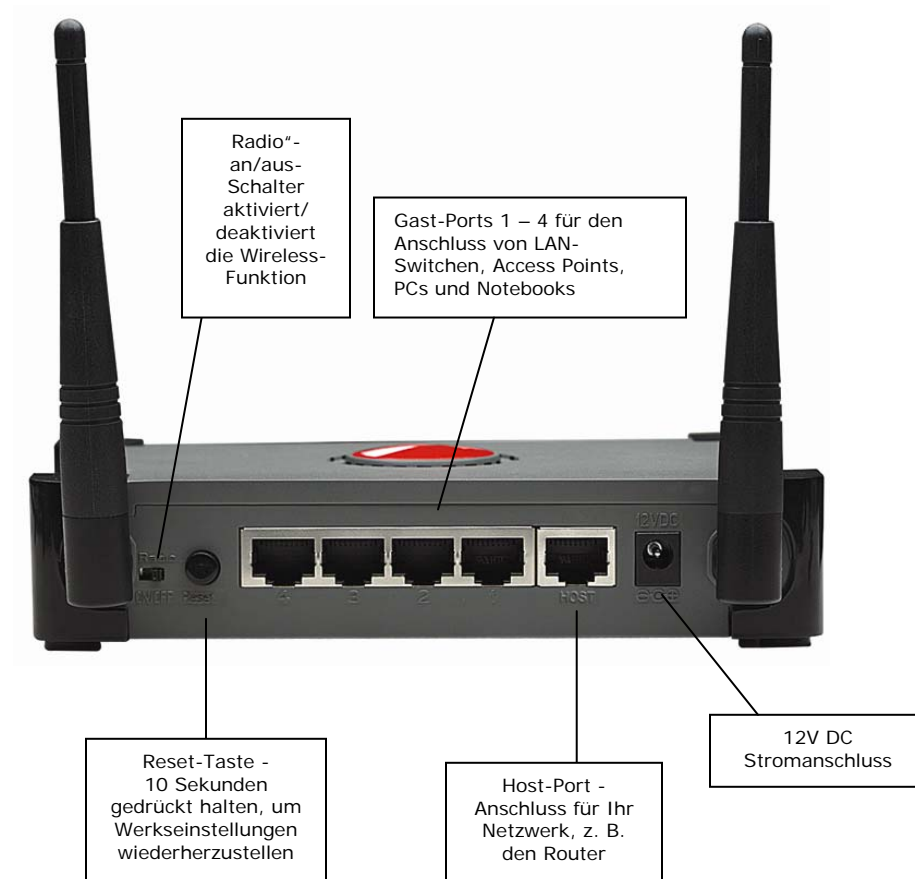
### **1. Verbindung mit dem Gastgeber-Netzwerk**

Verbinden Sie den HOST-Port des GuestGates über ein RJ-45-Netzkabel mit einem freien RJ-45 Port in Ihrem vorhandenen Netzwerk (z.B. Ethernet Switch Port, Router Switch Port, etc.). Schalten Sie das GuestGate ein und überprüfen Sie, dass die Netzwerkverbindung aktiv ist (HOST LED am GuestGate muss leuchten). *HINWEIS:* Der Startvorgang kann bis zu 30 Sekunden in Anspruch nehmen.

### **2. Verbindung Ihrer Gäste**

Über Standard-RJ45-Netzkabel können Sie PCs, Notebooks, Ethernet-Switches, Hubs oder Wireless Access Points an die Guest Ports von GuestGate anschließen. Jeder Port hat seine eigene Status-LED. Prüfen Sie, dass die Netzwerkverbindung auf jedem Port aktiv ist, mit dem Sie sich verbinden.

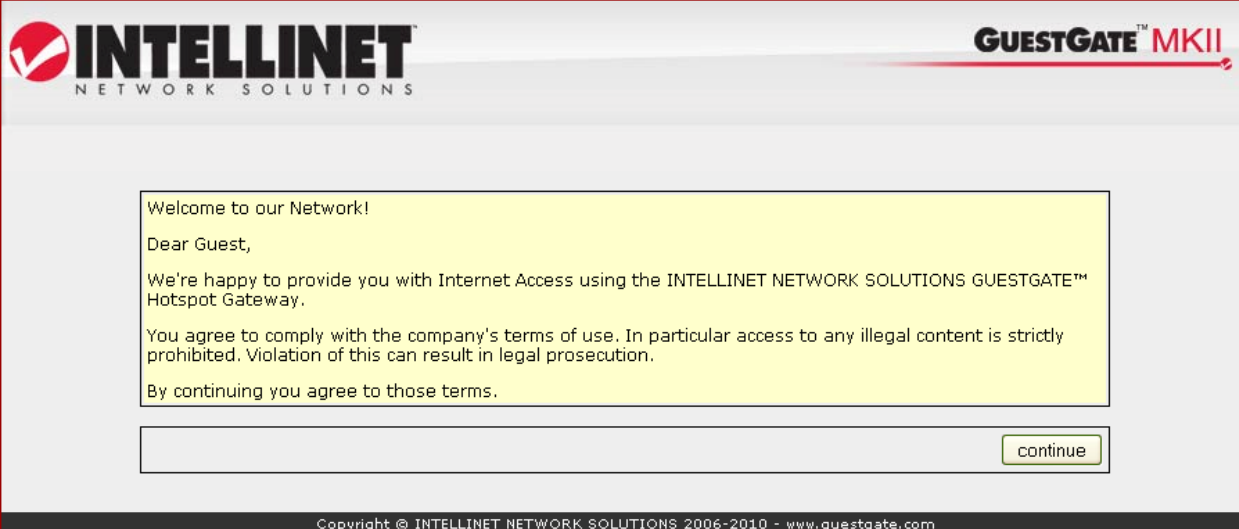
Alternativ können Sie GuestGate kabellos verbinden, über das Wireless Netzwerk mit dem Namen "GuestGate."



### 3. Internetzugang testen

Starten Sie einen PC oder Laptop, der mit einem der Guest Ports verbunden ist. Öffnen Sie Ihren Webbrowser und eine Internetseite z. B.  
<http://www.intellinet-network.com>.

Sie gelangen zunächst auf die GuestGate-Startseite/Willkommensseite.



**INTELNET**  
NETWORK SOLUTIONS

**GUESTGATE™ MKII**

Welcome to our Network!

Dear Guest,

We're happy to provide you with Internet Access using the INTELNET NETWORK SOLUTIONS GUESTGATE™ Hotspot Gateway.

You agree to comply with the company's terms of use. In particular access to any illegal content is strictly prohibited. Violation of this can result in legal prosecution.

By continuing you agree to those terms.

Copyright © INTELNET NETWORK SOLUTIONS 2006-2010 - [www.guestgate.com](http://www.guestgate.com)

Klicken Sie auf “Weiter” und Sie werden auf die Webseite weitergeleitet, die Sie ursprünglich in der Adresszeile eingegeben haben.

#### **Hinweis:**

Um Zugriff auf das Internet zu erhalten, muss zunächst ein Webbrowser gestartet und eine Webseite aufgerufen werden. Andere Anwendungen wie z.B. Chat-Programme (ICQ, MSN Messenger, Skype etc.) haben keine Internetverbindung, bevor die Startseite im Webbrowser bestätigt wurde.

#### 4. Zugriff auf das Administrator-Webinterface über das Gastgebernnetzwerk

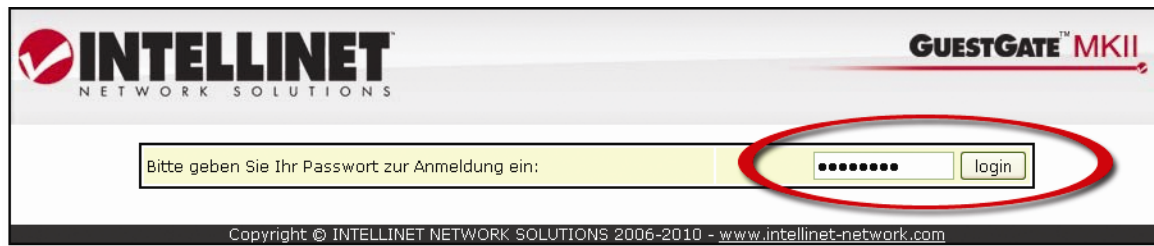
A. Verbinden Sie den Router (DHCP-Server) in Ihrem Netzwerk und öffnen Sie das DHCP-Client-Log des Routers. Schließen Sie den Host-Port des GuestGates an einen der LAN-Ports Ihres Routers an und starten Sie das GuestGate-Gerät. Warten Sie ca. 30 Sekunden und aktualisieren Sie dann das DHCP-Client-Log des Routers. Der letzte Eintrag (der neueste) gehört zu GuestGate.

Im Folgenden sehen Sie ein Beispiel einer DHCP-Log-Datei:

IP Address	MAC Address	Time Expired(s)
192.168.0.100	00:50:fc:be:48:58	169576
192.168.0.101	00:0f:a3:1d:a3:da	114749

B. Starten Sie Ihren Webbrowser und geben Sie in der Adresszeile die IP-Adresse ein, die im DHCP-Client-Log angezeigt wurde. Sie sehen dann das Administrator-Web-Interface.

Das Standardpasswort lautet: **1234**.



**Hinweis:** Falls dieser Vorgang nicht funktionieren sollte, kann dem Computer eine feste (statische) IP-Adresse im Bereich von 192.168.2.xxx zugewiesen werden, GuestGate vom Router getrennt und über den Host Port direkt mit dem Computer verbunden werden. Schalten Sie GuestGate ein und warten Sie ca. 60 Sekunden, bis die „Power“-LED aufhört zu blinken. Öffnen Sie dann die Standard-IP-Adresse von GuestGate (192.168.2.1) mit dem Webbrowser. Weitere Informationen erhalten Sie im Abschnitt „Erweiterte Einrichtung“.

## 5. Änderung des Administratorpassworts

Aus Sicherheitsgründen sollten Sie das Administratorpasswort von GuestGate ändern. Mit den folgenden Anweisungen können Sie das Passwort ändern.



Klicken Sie auf "Geräteeinstellungen".



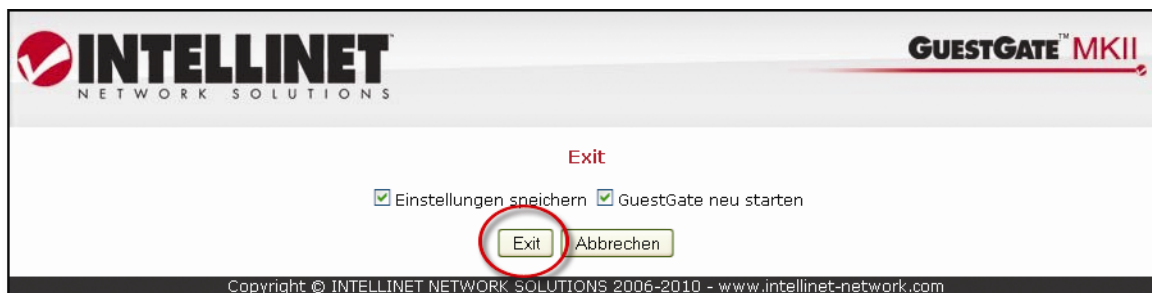
Geben Sie das aktuelle Passwort ein: 1234

Geben Sie ein neues Passwort ein (bis zu 20 Zeichen).

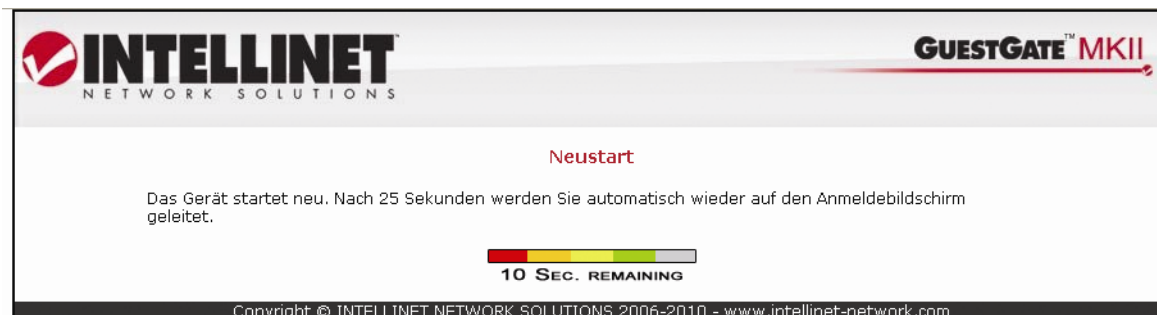
Bestätigen Sie das neue Passwort.

Klicken Sie auf "Passwort ändern".

Klicken Sie auf "Exit".



Setzen Sie ein Häkchen bei "Einstellungen speichern".  
Setzen Sie ein Häkchen bei "GuestGate neu starten".



Der Neustart dauert etwa 25 Sekunden nach denen sie auf die die Login-Seite von GuestGate weitergeleitet werden.

#### **HINWEIS:**

Die Benutzeroberfläche ist so angelegt, dass Sie Änderungen in allen Konfigurationsfenstern vornehmen können, ohne jedes Mal individuell speichern zu müssen. Sobald Sie die Einstellungen von GuestGate abgeschlossen haben, klicken Sie auf "Exit" und lassen Sie das Gerät neu starten.

Die Änderungen werden wirksam, nachdem GuestGate neugestartet wurde. Das Schließen des Webbrowsers ohne die Einstellungsänderungen zu speichern, hat den Verlust aller Änderungen zur Folge.

Waren die obigen Schritte erfolgreich, können Sie den nächsten Abschnitt überspringen.

## ***Erweiterte Einrichtung***

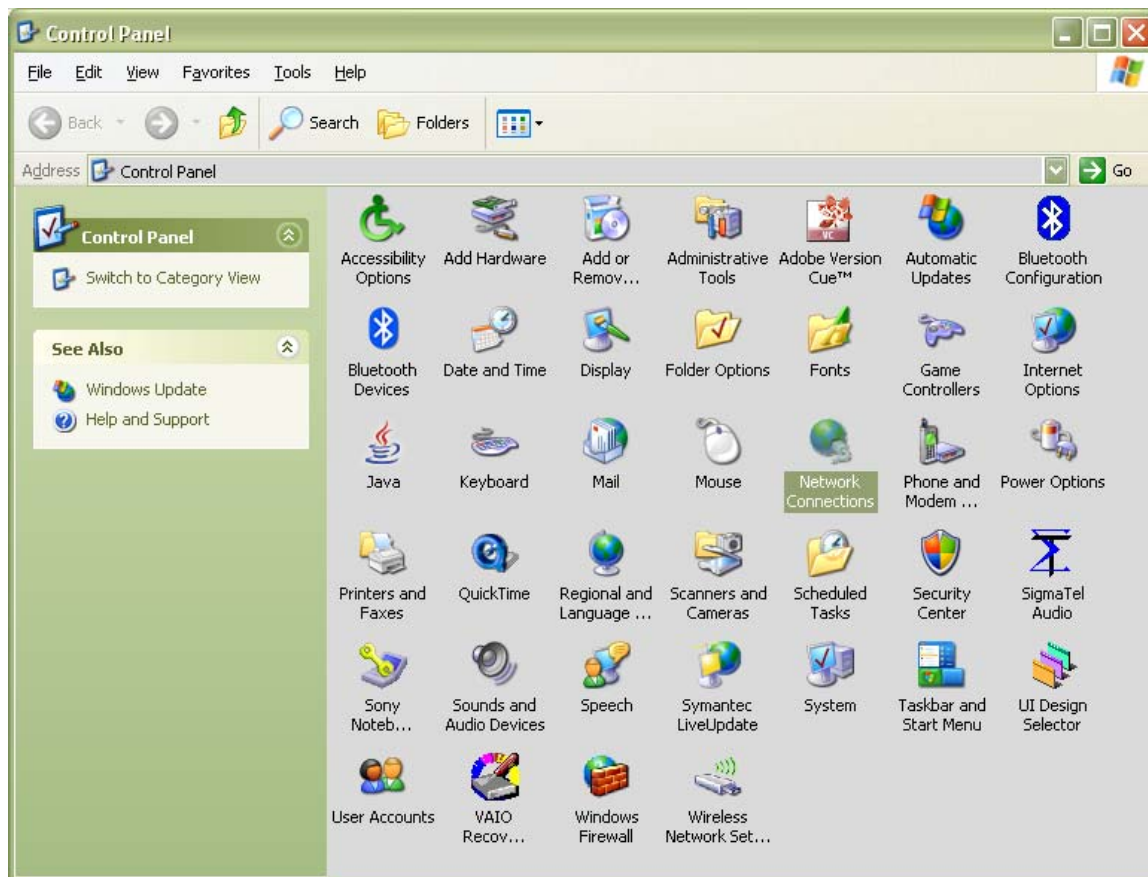
Die Standardinstallation des GuestGates geht von der Annahme aus, dass sich ein DHCP-Server in Ihrem Netzwerk befindet. Falls dies nicht der Fall ist, können Sie das GuestGate auch manuell konfigurieren. Hierfür schalten Sie das GuestGate ein, ohne es mit dem Netzwerk zu verbinden. Wenn innerhalb von 3 Minuten kein DHCP-Server gefunden wird, setzt GuestGate seine IP Adresse standardmäßig auf 192.168.2.1.

Für die erweiterte Einrichtung wird folgendes benötigt:

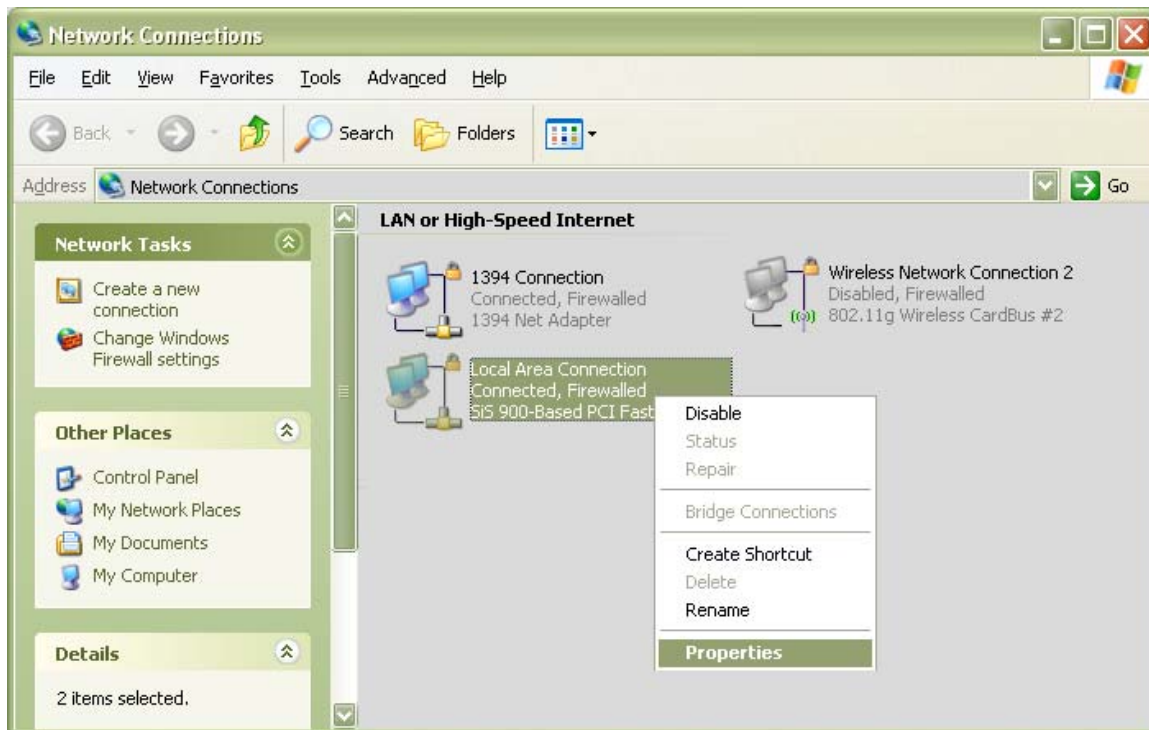
- Ein korrekt eingerichteter Netzwerkadapter an Ihrem Computer
- Benutzerrechte, die Ihnen erlauben, die TCP/IP Einstellungen an Ihrem PC manuell zu ändern
- GuestGate muss über ein RJ-45-Netzwerkkabel mit Ihrem Computer verbunden sein

### **1. Änderung der IP-Adresse Ihres PCs (Beispiel: Windows XP)**

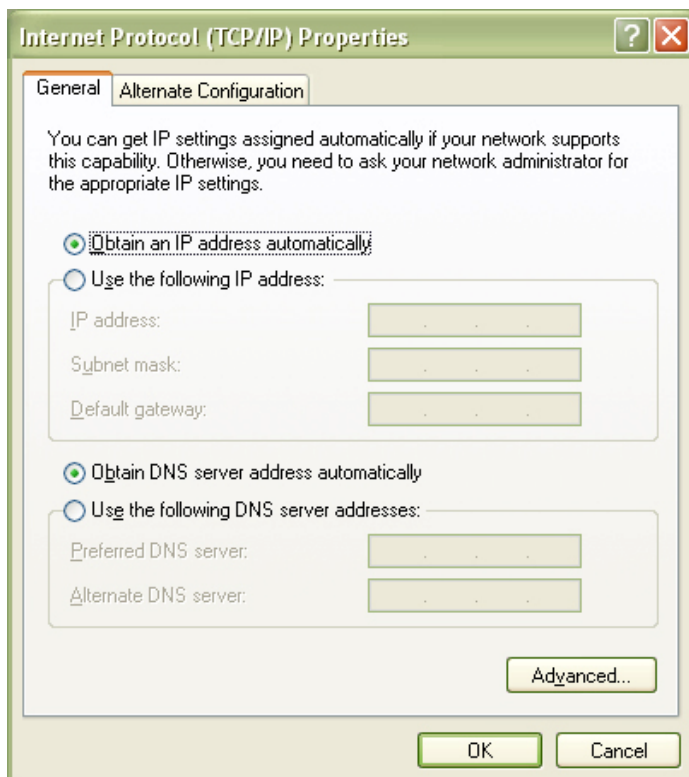
Klicken Sie auf „Start“ -> „Systemsteuerung“



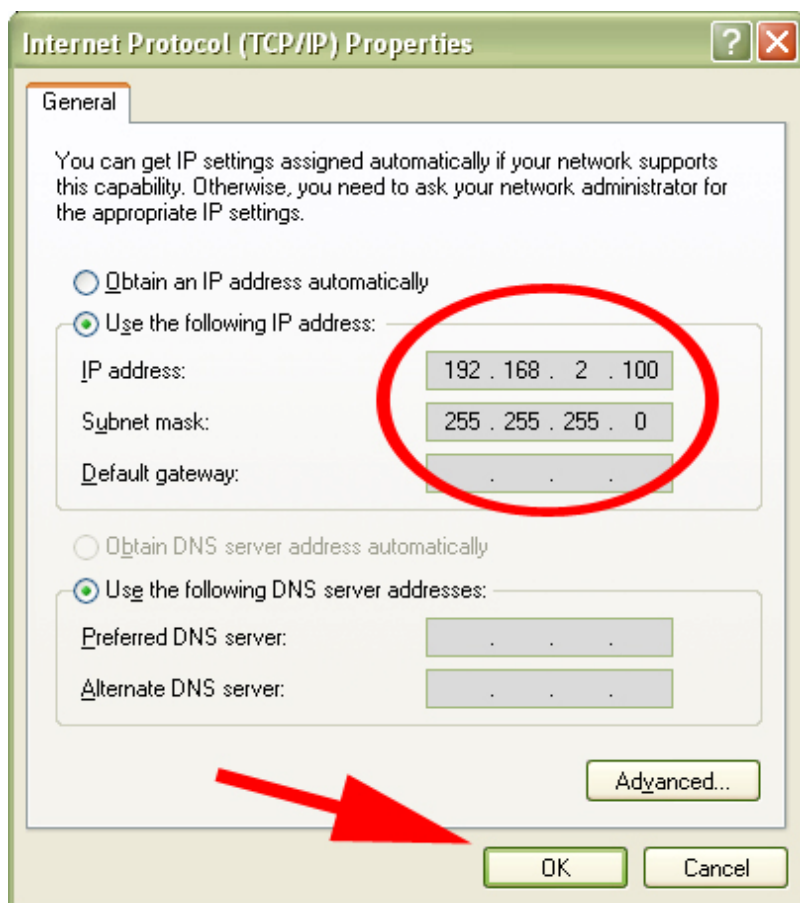
Doppelklicken Sie auf das “Netzwerkverbindungen”-Symbol.



Rechtsklicken Sie auf „LAN-Verbindung“ und im Kontextmenü auf „Eigenschaften“.  
 Im Fenster „Eigenschaften von LAN-Verbindung“ markieren Sie „Internetprotokoll (TCP/IP)“  
 und klicken Sie auf „Eigenschaften“.  
 Im Fenster „Eigenschaften von Internetprotokoll (TCP/IP)“ nehmen Sie folgende  
 Einstellungen vor:







Klicken Sie anschließend auf „OK“.

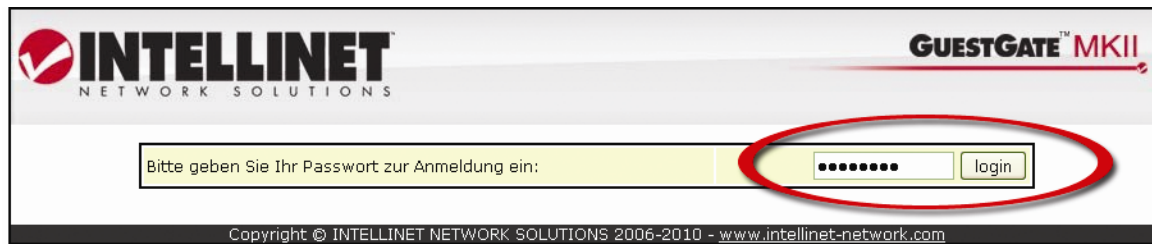
Schließen das vorherige Fenster, indem Sie erneut auf „OK“ klicken.

Die TCP/IP-Einstellungen Ihres Systems sind nun mit GuestGate kompatibel.



## 2. Mit GuestGate über einen Webbrowser verbinden

Öffnen Sie Ihren Webbrowser und geben Sie als Adresse ein: <http://192.168.2.1>.  
Das Login-Fenster des Administrator-Webinterface erscheint.



Geben Sie das Passwort **1234** ein und klicken Sie auf “Login”.

### **HINWEIS:**

Wir empfehlen, das Administratorpasswort wie im vorherigen Kapitel beschrieben zu ändern.

## 3. Gastgeber-Konfiguration



Netzwerk Informationen	
Host Netzwerk IP-Adresse:	67.111.35.58
Host Netzwerk Netzmaske:	255.255.192.0
Host Netzwerk Gateway:	67.111.35.1
Host Netzwerk DNS-Server:	65.106.1.196
Host Port MAC-Adresse:	00:0C:43:30:52:77
Gast Port MAC-Adresse:	00:0C:43:30:52:77

Geräteinformationen	
Firmware-Version:	1.25.10 (ralink3052)
Betriebszeit:	0 day(s), 00:01:23 (hh:mm:ss)
Zeit:	Error resolving pool.ntp.org.

Gerätestatus	
Passwortgeschützter Internetzugang:	aktiviert
Internetzugang für Gäste:	aktiviert <input type="button" value="deaktivieren"/>

Verbundene Gastcomputer		
MAC-Adresse	IP Adresse	Angemeldet

Klicken Sie auf „Gastgeber”.

<b>Gastgebernetz-Konfiguration:</b>	statisch <input type="button" value="v"/>	
IP Adresse:	<input type="text" value="67.111.35.58"/>	
IP Netzmaske:	255.255.192.0 <input type="button" value="v"/>	
IP Gateway:	<input type="text" value="67.111.35.1"/>	
DNS Server:	<input type="text" value="65.106.1.196"/>	
Administrator IP-Adresse:	<input type="text"/>	<input type="button" value="Die IP-Adresse dieses Computers verwenden"/>

Geben Sie in diesem Fenster die IP-Adresse, IP-Subnetzmaske, IP-Gateway (Internetverbindungsgateway, Router) und DNS-Server an.

IP-Adresse:

Eine freie IP-Adresse in Ihrem Netzwerk. Dies ist die IP-Adresse, die Sie GuestGate zuweisen.

IP Netzmaske:

Geben Sie dieselbe Netzmaske (oder Subnetzmaske) ein, die Sie in Ihrem Netzwerk verwenden.

IP Gateway:

Die IP-Adresse Ihres Internet-Gateways (z. B. Router).

DNS-Server:

Sie können mehrere DNS-Server eingeben, indem Sie die einzelnen Einträge mit einem Leerzeichen trennen.

Administrator-IP-Adresse:

Wenn angegeben, kann nur von dieser Adresse aus auf das Administratormenü des GuestGates zugegriffen werden. Durch die Funktion „Die IP-Adresse dieses Computers verwenden“ wird automatisch die IP-Adresse des momentan genutzten Computers in dem Feld hinterlegt.

Zum Beenden klicken Sie rechts oben auf „Exit“.

Klicken Sie auf „Exit“, um die Einstellungen zu speichern und GuestGate neuzustarten.

# EINSTELLUNGSOPTIONEN

## Statusseite

The screenshot shows the 'Gerätestatus-Informationen' page of the GuestGate interface. It features a navigation bar at the top with icons for Status, Gast, Gastgeber, Planer, Willkommenseite, Geräte-Einstellungen, and Exit. The main content area is divided into four sections:

- Netzwerk Informationen:** A table showing network details.

Host Netzwerk IP-Adresse:	67.111.35.58
Host Netzwerk Netzmaske:	255.255.192.0
Host Netzwerk Gateway:	67.111.35.1
Host Netzwerk DNS-Server:	65.106.1.196
Host Port MAC-Adresse:	00:0C:43:30:52:77
Gast Port MAC-Adresse:	00:0C:43:30:52:77
- Geräteinformationen:** A table showing device details.

Firmware-Version:	1.25.10 (ralink3052)
Betriebszeit:	0 day(s), 00:03:14 (hh:mm:ss)
Zeit:	Error resolving pool.ntp.org.
- Gerätestatus:** A table showing the status of password protection and internet access.

Passwortgeschützter Internetzugang:	aktiviert
Internetzugang für Gäste:	aktiviert <a href="#">deaktivieren</a>
- Verbundene Gastcomputer:** A table header for connected guest computers.

MAC-Adresse	IP Adresse	Angemeldet
-------------	------------	------------

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - [www.intellinet-network.com](http://www.intellinet-network.com)

**1. Netzwerkinformationen:** Basisinformationen über das Gastgebernetzwerk-Interface.

**2. Geräteinformationen:** Zeigen die aktuelle Firmwareversion, die Betriebszeit des Systems und Systemzeit.

### 3. Gerätestatus

Zeigt den Status des Passwortschutzes ("deaktiviert" = kein Passwort benötigt) und den Status des Internetzugangs ("aktiviert" = Internetzugang ist aktiv).

### 4. Verbundene Gastcomputer

GuestGate zeigt alle verbundenen Gastcomputer, einschließlich deren MAC-Adressen, zugewiesenen IP-Adressen und deren Verbindungszeit. Klicken Sie auf "Details", um individuelle Statistiken für jeden verbundenen PC anzuzeigen, einschließlich deren verbrauchter Bandbreite (Mbyte). Klicken Sie auf "Disconnect (Trennen)", um die Verbindung zum ausgewählten Computer zu unterbrechen. Werden bei „Angemeldet“ keine Informationen angezeigt, hat sich der Nutzer bei GuestGate angemeldet, aber noch nicht die Startseite bestätigt.

Verbundene Gastcomputer			
MAC-Adresse	IP Adresse	Angemeldet	
00:23:4e:92:b4:39	192.168.11.94	0 day(s), 02:31:48 (hh:mm:ss)	<a href="#">Disconnect</a> <a href="#">Details</a>
00:23:4e:92:b3:9d	172.17.117.114		<a href="#">Disconnect</a> <a href="#">Details</a>
00:13:02:a6:df:0c	10.28.78.214		<a href="#">Disconnect</a> <a href="#">Details</a>

## Gast-Konfigurationsseite

Status
 Gast
 Gastgeber
 Planer
 Willkommenseite
 Geräte-Einstellungen
 Exit

### Gast-Konfiguration

**Gast-Konfiguration:** Separates Netzwerk für jeden Benutzer

IP Adresse: 172.16.254.254

IP Netzmaske: 255.255.255.0

Dynamischer Bereich: 172.16.254.1 bis 172.16.254.253

**Zugriffskontrolle: Wireless LAN**

Wireless LAN: aktiviert

SSID: INTELLINET

Wireless Modus: 802.11 B/G/N

Kanal-Nummer: 2

**Zugriffskontrolle: Grundeinstellungen**

Limit Download-Bandbreite: unbegrenzt

Limit Upload-Bandbreite: unbegrenzt

Vertrauenswürdige MAC-Adressen: 00:1f:1f:7a:b1

MAC Adresse hinzufügen:

**Zugriffskontrolle: Willkommenseite**

Willkommenseite: aktiviert

Globales Gast Passwort: •••••• (leer lassen um Passwort zu deaktivieren)

RADIUS Server: (leer lassen um RADIUS zu deaktivieren)

RADIUS Passwort:

RADIUS Realm:

**Zugriffskontrolle: Individuelle Passwörter**

Passwort	Gültig von	Gültig bis	Maximale Anzahl Benutzer	
andy	04/02/2010 00:00	04/05/2010 16:00	1	
<input type="text"/>	<input type="text"/> 0:00 (12am)	<input type="text"/> 0:00 (12am)	-	

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - [www.intellinet-network.com](http://www.intellinet-network.com)

Diese Seite zeigt die Einstellungsoptionen für verbundene Gastcomputer

### 1. Gast-Konfiguration

#### Option "Separates Netzwerk für jeden Benutzer"

Ist diese Option aktiviert, weist GuestGate jedem verbundenen Gastcomputer ein zufällig generiertes Netzwerk zu. Diese Option sollte aktiviert sein, wenn Sie verhindern möchten, dass sich Gastcomputer gegenseitig „sehen“ und aufeinander zugreifen können. (Layer 3 Client Isolation = an). Standardmäßig aktiviert.

### 2. Option „Alle Benutzer operieren im selben Netzwerk (automatisch)“

GuestGate vergibt automatisch IP-Adresse an die Gastcomputer. Alle Gastcomputer operieren in demselben Netzwerk (Layer 3 Client Isolation = aus).

#### Option "Alle Benutzer operieren im selben Netzwerk (manuell)"

Ist diese Option aktiviert, können Sie das Netzwerk für verbundene Gastcomputer manuell festlegen (Layer 3 Client Isolation = aus).

### 3. Zugriffskontrolle: Wireless LAN

#### Wireless LAN

Ermöglicht die Aktivierung oder Deaktivierung der WLAN-Funktion von GuestGate.

#### SSID

Legen Sie den Namen des Wireless Netzwerks fest, z. B., "free wifi", "gast wireless", "hotelwifi", etc.

#### Wireless Modus

Hier können Sie auswählen, welche Wireless Modi von GuestGate unterstützt werden. Der Standardmodus ist 802.11 B/G/N. Er unterstützt die älteren Wireless-B und Wireless-G-Standards ebenso wie den neuen Wireless-N-Standard von 300 Mbit/s. Für optimale Kompatibilität empfehlen wir den standardmäßigen B/G/N Modus



#### Kanalnummer

Setzen Sie GuestGate auf einen Kanal zwischen 1 und 11. Um in Ihrem Wireless LAN die maximale Performance zu erreichen, sollten Sie den Kanal mit größtmöglichem Unterschied zu anderen Netzwerken in Ihrer Umgebung wählen. Befindet sich dort zum Beispiel ein Netzwerk mit dem Kanal 4, sollten Sie GuestGate nicht auf 4, 5 oder 6 setzen, sondern auf 7 oder höher.

### 4. Zugriffskontrolle: Grundeinstellungen

Bandbreitenbegrenzung und vertrauenswürdige Ethernet-Adressen.



#### Bandbreiten-Download-Limit

Kontrollieren Sie die maximale Downloadgeschwindigkeit, die den verbundenen Gastcomputern zur Verfügung steht. Mögliche Einstellungen reichen von 32 Kbit/s (Kilobit pro Sekunde) bis 2048 Kbit/s (= 2 Megabit pro Sekunde). Standard = unbegrenzt.

#### Bandbreiten-Upload-Limit

Bandbreitenbegrenzung für die Upload-Geschwindigkeit (Versenden von Dateien), mit

den gleichen Optionen wie bei der Download-Begrenzung.

### Vertrauenswürdige Ethernet-Adressen

Möchten Sie einen Gastcomputer permanent authentifizieren, können Sie seine MAC-Adresse zur GuestGate-Konfiguration hinzufügen. Diesen Computern wird die "Willkommen"-Seite nicht mehr angezeigt. Geben Sie die MAC-Adresse des Computers wie oben beschrieben ein. Das Format lautet xx:xx:xx:xx:xx:xx. Klicken Sie auf „Hinzufügen“, um die MAC-Adressen zu speichern. Wiederholen Sie diese Schritte für weitere MAC-Adressen. Um eine MAC-Adresse aus der Konfiguration zu löschen, wählen Sie den entsprechenden Eintrag im Dropdown-Menü aus und klicken Sie auf „Entfernen“.


<b>Vertrauenswürdige MAC-Adressen:</b>	00:1f:1f:1f:7a:b1 ▼	Entfernen
MAC Adresse hinzufügen:	<input type="text"/>	Hinzufügen

Sie können die MAC-Adresse eines verbundenen Computers im GuestGate-Statusfenster folgendermaßen in Erfahrung bringen (Beispiel: Windows 2000/XP/Vista/Windows 7): Klicken Sie auf „Start“ => Ausführen, geben Sie **cmd** ein, drücken Sie **Enter**, dann geben Sie **ipconfig/all** ein und drücken Sie **Enter**.

### **Beispiel:**

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : 802.11g Wireless CardBus
Physical Address. . . . . : 00-0F-A3-1D-A3-DA
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.10.10.89
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 10.10.8.1
DHCP Server . . . . . : 10.10.8.10
DNS Servers . . . . . : 10.10.8.10
                        10.10.8.21
```



Die **PHYSIKALISCHE ADRESSE** ist die MAC-Adresse, die in der Konfiguration von GuestGate eingegeben werden muss.

Das Format lautet: xx:xx:xx:xx:xx:xx (nicht xx-xx-xx-xx-xx-xx)

## 5. Zugriffskontrolle: Start-/Willkommenseite

### Willkommenseite

Hier aktivieren bzw. deaktivieren Sie die Willkommenseite für Gäste. (Standard = aktiviert). Ist die Willkommenseite deaktiviert, wird der Internetzugang automatisch gewährt. Es wird keine Willkommenseite angezeigt, auch wenn ein Gastpasswort vergeben ist.

### Globales Gastpasswort:

Wenn Sie Ihre Gäste auffordern möchten, ein Passwort einzugeben, um Internetzugang zu erhalten, dann können Sie dieses hier festlegen. Bleibt das Feld leer, wird kein Passwort abgefragt. (Standard = kein Passwort). Dies ist das globale Passwort, das von jedem Gast benutzt werden kann. Es ist kein individuelles Benutzerpasswort. Die Passwort-Option ist nur aktiv, wenn die Willkommenseite aktiviert ist.

### Radius-Server:

Haben Sie einen Radius-Authentifizierungsserver in Ihrem Netzwerk und Sie möchten ihn zur Authentifizierung Ihrer Gastnutzer verwenden, können Sie die IP-Adresse des Servers hier eingeben.

### Radius-Passwort:

Geben Sie das optionale Passwort für den Radius-Server hier ein.

### Radius Realm:

Geben Sie den optionalen Realm Delimiter hier ein (z. B. „@“ oder „\“).

## 6. Zugriffskontrolle: Individuelle Passwörter

Legen Sie individuelle Benutzerpasswörter fest, die nur für eine gewisse Zeitspanne wirksam sind und von einer festgelegten Anzahl Nutzern gleichzeitig verwendet werden können. Das unten stehende Beispiel zeigt das Passwort „test“, das vom „28.05.2010, 24 Uhr“ bis „02.06.2010, 24 Uhr gültig ist“. Das Passwort kann nur von einem Nutzer gleichzeitig verwendet werden. Im Feld darunter könnten Sie die Anzahl der gleichzeitigen Nutzer auswählen. Die Anzahl der Benutzerpasswörter ist durch den verfügbaren Speicherplatz in GuestGate festgelegt, aber sollte idealerweise 20 nicht übersteigen.

Zugriffskontrolle: Individuelle Passwörter				
Passwort	Gültig von	Gültig bis	Maximale Anzahl Benutzer	
andy	04/02/2010 00:00	04/05/2010 16:00	1	Entfernen
<input type="text"/>	<input type="text"/> 0:00 (12am) ▼	<input type="text"/> 0:00 (12am) ▼	- ▼	Hinzufügen

## Gastgeber-Konfigurationsseite

**Gastgebernnetz-Konfiguration**

Gastgebernnetz-Konfiguration: statisch

IP Adresse: 192.168.2.2

IP Netzmaske: 255.255.255.0

IP-Netzmaske: 192.168.2.1

DNS Server: 192.168.2.1

Administrator IP-Adresse:

**Paket Filter**

Gesperrte Adressen: ☒ Entfernen

Host Adresse hinzufügen:

Netzwerk Adresse hinzufügen:  / 255.255.255.0 ☒

Geblockte Ports: ☒ Entfernen

Port Nummer hinzufügen:

Erlaubte Adressen: 10.10.8.21 ☒ Entfernen

Host Adresse hinzufügen:

Netzwerk Adresse hinzufügen:  / 255.255.255.0 ☒

Walled Garden Adressen: ☒ Entfernen

Host Adresse hinzufügen:

Netzwerk Adresse hinzufügen:  / 255.255.255.0 ☒

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - [www.intellinet-network.com](http://www.intellinet-network.com)

### 1. Gastgebernnetz-Konfiguration

#### Einstellung "DHCP"

GuestGate bezieht automatisch IP-Adresse, Netzmaske, Gateway und DNS-Server von dem DHCP-Server, üblicherweise ein Router, Ihres Netzwerks.

#### Einstellung "statisch"

In größeren Netzwerken kann eine manuelle Konfiguration der IP-Einstellungen notwendig sein. Wählen Sie "statisch" und geben Sie IP-Adresse, Netzmaske, Gateway IP-Adresse und DNS-Server manuell ein. Es können mehrere DNS-Server angegeben werden, die durch ein Leerzeichen getrennt werden, z.B.

111.222.333.444 999.888.777.666.

#### Administrator-IP-Adresse:

Beschränken Sie den Administratormenü-Zugriff auf die hier angegebene IP-Adresse. Es kann sich dabei um eine lokale oder öffentliche IP-Adresse handeln.



## 2. Paketfilter

### Gesperrte Adressen

Möchten Sie bestimmte IP-Adressen, Domain-Namen oder ein ganzes Netzwerk sperren, können Sie diese hier eingeben. „Host-Adresse hinzufügen“ wird verwendet, um Domain-Namen wie `guestgate.com` oder `intellinet-network.com` einzugeben. Geben Sie den Domain-Namen ein und klicken Sie auf „Host hinzufügen“. Wiederholen Sie diese Schritte, um weitere Domains zu sperren. „Netzwerkadresse hinzufügen“ wird verwendet, um eine IP-Adresse einzugeben. Um den Adressbereich festzulegen, können Sie die entsprechende Netzmaske aus der Drop-down-Liste auswählen. Um eine gesperrte Adresse zu löschen, wählen Sie sie aus der Drop-down-Liste und klicken Sie auf „Entfernen“.

Paket Filter			
Gesperrte Adressen:	<input type="text" value="theiratebay.org"/>	<input type="button" value="Entfernen"/>	
Host Adresse hinzufügen:	<input type="text" value="theiratebay.org"/>	<input type="button" value="Host hinzufügen"/>	
Netzwerk Adresse hinzufügen:	<input type="text" value="74.125.157.104"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Netzwerk hinzufügen"/>

### Gesperrte Ports

Hier legen Sie fest, welche ausgehenden TCP/IP Ports Sie sperren möchten. Geben Sie die Port-Nr. ein und klicken Sie auf „Port hinzufügen“. GuestGate sperrt sowohl TCP- als auch UDP-Protokolle. Eine Liste gängiger Service-Ports finden Sie im Abschnitt -> [ANHANG](#) am Ende dieses Handbuchs. Um einen Port zu entfernen, wählen Sie diesen einfach im Drop-down-Menü aus und klicken Sie auf „Entfernen“  
**Hinweis:** Sie können nur einzelne Ports hinzufügen oder entfernen. Ganze Port-Bereiche werden nicht unterstützt.

### Freigegebene (erlaubte) Adressen

Standardmäßig verweigert GuestGate den Zugriff auf alle PCs im Host (Gastgeber)-Netzwerk. Hier können Sie Ausnahmen festlegen.

Host-Adresse hinzufügen: Geben Sie hier eine einzelne IP-Adresse ein, z.B. die IP-Adresse Ihres Intranet-Webserver und klicken Sie auf Host hinzufügen. Wiederholen Sie diesen Vorgang, wenn Sie weitere IP-Adressen eingeben möchten.

Erlaubte Adressen:	<input type="text" value="10.10.8.21"/>	<input type="button" value="Entfernen"/>
Host Adresse hinzufügen:	<input type="text" value="10.10.8.22"/>	<input type="button" value="Host hinzufügen"/>

Das obenstehende Beispiel zeigt, dass der Zugriff auf die IP-Adresse 10.10.8.21 gewährt wird. Zugriff auf die IP-Adresse 10.10.8.22 wird gewährt, sobald Sie auf „Host hinzufügen“ klicken.

Netzwerkadresse hinzufügen: Geben Sie hier eine IP-Adresse und Netzmaske ein, um einen ganzen IP-Adressbereich für Ihre Gäste freizugeben. Möchten Sie z. B. Zugriff auf das gesamte Host-Netzwerk erlauben, können Sie folgende Funktion nutzen:

Netzwerk Adresse hinzufügen:	<input type="text" value="10.10.8.1"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Netzwerk hinzufügen"/>
------------------------------	--	--	--

Das obige Beispiel zeigt, wie Sie den Zugriff auf den gesamten Netzwerkbereich von 10.10.8.1 bis 10.10.8.254.

### Walled-Garden-Adressen

Mit der Walled-Garden-Funktion können Sie einem nicht-authentifizierten Nutzer begrenzten Zugang auf interne und externe Webseiten erlauben. Die Adressen dieser Webseiten können Sie selbst festlegen und dieser Bereich wird dann Walled Garden genannt und jeder Nutzer hat auf diese Seiten Zugriff, ob dieser eingeloggt ist oder nicht.

Sobald der Nutzer versucht, eine Adresse außerhalb des Walled Garden zu öffnen, verlangt GuestGate eine Authentifizierung, siehe unten:



#### Internet

Authentifizierung für Zugang benötigt

#### Walled Garden

Zugang ohne Authentifizierung





Welcome to our Network!

Dear Guest,

We're happy to provide you with Internet Access using the INTELLINET NETWORK SOLUTIONS GUESTGATE™ Hotspot Gateway.

You agree to comply with the company's terms of use. In particular access to any illegal content is strictly prohibited. Violation of this can result in legal prosecution.

By continuing you agree to those terms.

Password:

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - [www.intellinet-network.com](http://www.intellinet-network.com)

Die Walled-Garden-Funktion in Kombination mit einer individuellen Willkommensseite (siehe nächster Abschnitt) erlaubt Gästen Zugriff auf Webseiten Ihrer Wahl, ohne dass Sie dafür ein Passwort zur Verfügung stellen müssen. Die Startseite könnte folgendermaßen aussehen:

Welcome to our Network!

Dear Guest,

We're happy to provide you with Internet Access using the INTELLINET NETWORK SOLUTIONS GuestGate™ Hotspot Gateway.

You agree to comply with the company's terms of use. In particular access to any illegal content is strictly prohibited. Violation of this can result in legal prosecution. By continuing you agree to those terms.

As password is required in order to access the Internet. You can obtain the password at the reception desk. In the meantime, you are welcome to browse through our special offers and services:

- [Hotel Service Numbers](#)
- [How to obtain Internet Access](#)
- [Our special offers](#)

Password:

Geben Sie die URLs und IP-Adressen in den Walled-Garden-Einstellungen ein. Auf diese können Ihre Gäste zugreifen, ohne dass sie dafür ein Passwort benötigen.

**Walled Garden Adressen:**

Host Adresse hinzufügen:

Netzwerk Adresse hinzufügen:  /

Host-Adresse hinzufügen: Geben Sie eine beliebige Webseiten-URL ein, die Sie zum „Walled Garden“ hinzufügen möchten. Klicken Sie dann auf „Host hinzufügen“.

Netzwerkadresse hinzufügen: Zusätzlich zu URLs, können Sie auch IP-Adressen zum „Walled Garden“ hinzufügen. Geben Sie IP-Adresse und Netzmaske ein und klicken Sie dann auf „Netzwerk hinzufügen“.

Um eine Walled-Garden-Adresse hinzuzufügen, wählen Sie die URL aus der Drop-down-Liste und klicken Sie dann auf „Entfernen“.

## Konfiguration der Willkommenseite

Willkommenseiten-Konfiguration

Erste Anfänge an folgenden URL umleiten:

Modus um die Willkommenseite anzupassen:

**Banner Grafik**

Banner:

Eigenes Bild hochladen:

**Willkommenseiten-Text**

Welcome to our Network!

Dear Guest,

We're happy to provide you with Internet Access using the INTELLINET NETWORK SOLUTIONS GUESTGATE™ Hotspot Gateway.

You agree to comply with the company's terms of use. In particular access to any illegal content is strictly prohibited. Violation of this can result in legal prosecution.

By continuing you agree to those terms.

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - www.intellinet-network.com

### 1. Erste Anfänge an folgende URL umleiten:

Wenn sich ein Gast zum ersten Mal mit GuestGate verbindet, kann GuestGate ihn zu einer Webseite Ihrer Wahl weiterleiten, z. B. Seiten mit Werbung oder Spezialangeboten.

### 2. Modus, um die Willkommenseite anzupassen:

Sie können aus zwei Werten auswählen: "einfach" und "erweitert". Im einfachen Modus können Sie den Willkommenstext ändern und die Standard-Bannergrafik ersetzen, im erweiterten Modus haben Sie Zugriff auf den gesamten HTML-Quellcode der Willkommenseite. Sobald Sie den erweiterten Modus aktivieren, erscheint ein zusätzliches Textfeld unten auf der Seite (siehe folgender Abschnitt: „HTML-Code der Willkommenseite“).

### 3. Bannergrafik

Sie können das Standard-Banner durch Ihr eigenes Banner, z.B. das Logo Ihres Unternehmens, ersetzen. Klicken Sie auf Browse (Durchsuchen), um eine Datei auszuwählen und auf „hochladen“, um diese zu verwenden. Nach dem Upload wechselt die Anzeige "Standard-Bild" zu "Eigenes Bild".

#### **Hinweis:**

Folgende Dateiformate werden unterstützt: JPG, GIF und PNG. Die Dateigröße darf 60 KB nicht überschreiten. Die Abmessungen sind nicht beschränkt, sollten aber idealerweise eine Breite von 1024 Pixel nicht übersteigen. Das Banner wird nur auf der Willkommenseite angezeigt, es ersetzt nicht das Banner im Administrator-Webinterface.

#### 4. Willkommenstext

Sie können den Standardtext einfach mit Ihrem eigenen überschreiben. GuestGate unterstützt HTML-Tags, um den Text zu formatieren. Unten sehen eine kleine Auswahl:

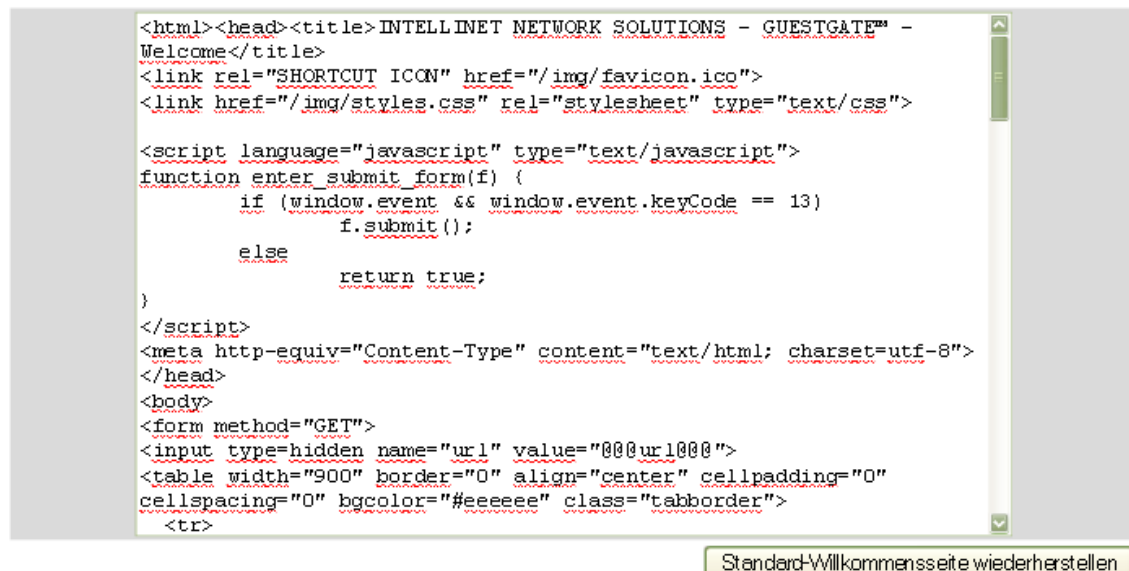
```
<strong>bold text</strong>
<font color = red>red text</font>
<font color = #00ff00>green text</font>
<u>underlined text</u>
<u><strong><font color = red>red bold underlined text</font></strong></u>
```

Andere HTML-Befehle wie <TABLE> <tr> <td> <img> und viele weitere werden ebenfalls unterstützt.

#### 5. HTML-Code der Willkommenseite

Wenn Sie den erweiterten Modus aktivieren, erscheint ein neues Textfeld. Diese Funktion ist für fortgeschrittene Nutzer mit HTML-Kenntnissen geeignet und auch nur für diese empfohlen.

##### HTML-Code der Willkommenseite



```
<html><head><title>INTELLINET NETWORK SOLUTIONS - GUESTGATE™ -  
Welcome</title>  
<link rel="SHORTCUT ICON" href="/img/favicon.ico">  
<link href="/img/styles.css" rel="stylesheet" type="text/css">  
  
<script language="javascript" type="text/javascript">  
function enter_submit_form(f) {  
    if (window.event && window.event.keyCode == 13)  
        f.submit();  
    else  
        return true;  
}  
</script>  
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">  
</head>  
<body>  
<form method="GET">  
<input type="hidden" name="url" value="@@@url@@@">  
<table width="900" border="0" align="center" cellpadding="0"  
cellspacing="0" bgcolor="#eeeeee" class="tabborder">  
<tr>
```

Standard-Willkommenseite wiederherstellen

Innerhalb des Textfelds befindet sich der gesamte HTML-Code der Willkommenseite. Möchten Sie Bilder eines externen Webserver einbetten, stellen Sie sicher, dass Sie den Webserver als Walled-Garden-Adresse übernommen haben. Der Standard-HTML-Code kann über die Schaltfläche rechts unten wiederhergestellt werden.

##### Hinweis:

Nehmen Sie Änderungen vor, achten Sie besonders auf Variablen wie “@@@WELCOME\_MSG@@@” sowie Java-Skripte und Formularelemente. Änderungen an diesen können zu ungewollten Ergebnissen führen.

## Zeit /Planer-Konfiguration

Status
 Gast
 Gastgeber
 Planer
 Willkommenseite
 Geräte-Einstellungen
 Exit

### Zeit / Planer

**Zeit Setup**

Zeitzone:

Aktualisieren:

GuestGate neu starten:

**Internet Zugangszeit Planer**

Internetzugang:

	all	S ON	MON	DIE	MIT	DON	FRE	S AM
0 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - [www.intellinet-network.com](http://www.intellinet-network.com)

### 1. Zeit Setup (Zeitzone und Häufigkeit der Aktualisierung)

Wählen Sie die Zeitzone, in der Sie sich befinden. Im Feld darunter können Sie festlegen, wie häufig sich GuestGate mit der Internetzeit synchronisiert.

### 2. GuestGate neu starten

Mit dieser Einstellung können Sie GuestGate einen täglichen Neustart durchführen lassen, zu einer Uhrzeit Ihrer Wahl. Haben Sie viele GuestGate-Nutzer, dann ist dieses Feature nützlich, um die Systemstabilität zu verbessern. Ebenso können Sie es nutzen, um alle Nutzer dazu zu bringen, sich zu einer bestimmten Zeit neu zu authentifizieren.

### 3. Internet Zugangszeit Planer

#### Internet Zugangszeit Planer

Internetzugang:	gemäß Zeitplan ▼							
	all	SON	MON	DIE	MIT	DON	FRE	SAM
0 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3 h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 h	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5 h	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6 h	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sie können festlegen, ob Internetzugang ständig verfügbar ist oder nur zu bestimmten Zeiten, z. B. während der Geschäftszeiten.

Einstellung "immer aktiv":

Internetzugang steht 24/7 zur Verfügung, ohne Einschränkungen.

Einstellung „gemäß Zeitplan“:

Mit dieser Option können Sie festlegen an welchen Tagen und zu welcher Uhrzeit Internetzugang zur Verfügung steht. Klicken Sie auf die Felder, um Internetzugang am entsprechenden Tag oder zur entsprechenden Uhrzeit zu aktivieren/deaktivieren. Mit Klick auf die Schaltflächen "SON", "MON" etc. können Sie den Zugang für den jeweiligen Tag ein- bzw. ausschalten. Das gleiche gilt für Uhrzeiten. Klicken Sie auf "4 h", um Internetzugang für jeden Tag von 4:00Uhr bis 5:00Uhr ein- bzw. auszuschalten. Klicken Sie auf "19 h" um Internet Zugang für jeden Tag von 19:00Uhr bis 20:00Uhr ein- bzw. auszuschalten. Die Schaltfläche „all“ aktiviert bzw. deaktiviert alle Felder.

#### Hinweis:

Wenn Sie den Zeitplaner nutzen, stellen Sie sicher, dass GuestGate Zugang zu einem NTP-Server hat. Prüfen Sie die Statusseite, um sicherzustellen, dass GuestGate eine korrekte Zeit erhalten hat. Ist dies nicht der Fall, steht kein Internetzugang zur Verfügung so lange der Zeitplaner aktiviert ist.

## Geräte-Einstellungen

**Geräte-Einstellungen**

**Administrator Passwort**

Aktuelles Passwort:

Neues Passwort:

Neues Passwort wiederholen:

**Sprache**

Sprache:

**Log-Datei**

aktiviert:

Sitzungen Log-Datei:

Datenverkehr Log-Datei:

**Konfiguration**

Konfigurationsdaten laden:

**Firmware**

Firmware aktualisieren:

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2010 - www.intellinet-network.com

Diese Seite ermöglicht das Ändern des Administratorpassworts, das Speichern und Wiederherstellen der Konfiguration sowie die Aktualisierung der Firmware.

### 1. Administrator-Passwort

Um das Administrator-Passwort zu ändern, müssen Sie das alte und neue Passwort eingeben und das neue zusätzlich bestätigen, indem Sie es erneut eingeben. Klicken Sie auf „Passwort ändern“, um die Änderungen zu speichern.

GuestGate-Standardpasswort: 1234

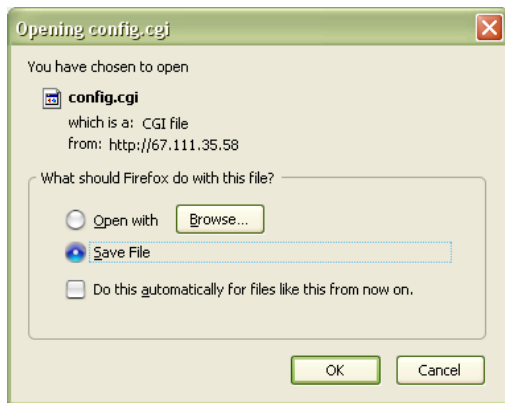
Das Passwort kann bis zu 20 Zeichen enthalten. Ein sicheres Passwort ist mindestens sieben Zeichen lang und enthält sowohl Buchstaben als auch Ziffern.

### 2. Log-Datei

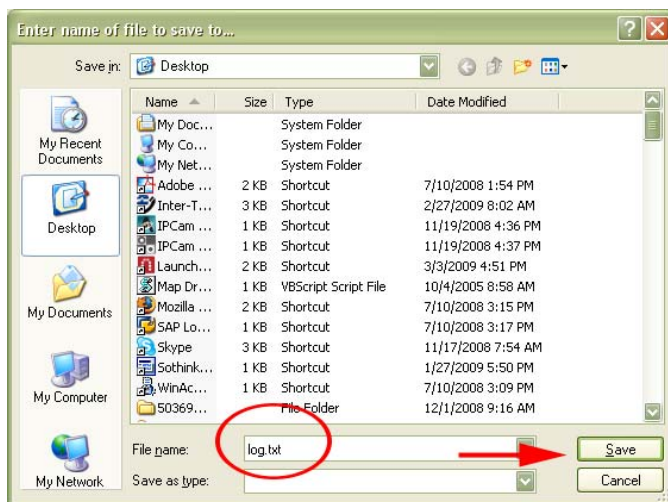
GuestGate kann ein Protokoll führen, das Informationen enthält wie Login-Datum und -Uhrzeit sowie Logout-Zeit, die IP-Adressen und die MAC-Adressen der verbundenen Computer (Session Log) oder auf welche Webseiten Gastcomputer zugegriffen haben (Traffic Log). Möchten Sie diese Vorgänge aufzeichnen, setzen Sie die Einstellung auf „aktiviert“.

Sie können die Log-Datei jederzeit herunterladen, indem Sie auf die entsprechende Schaltfläche klicken. Es öffnet sich folgendes Pop-up-Fenster:



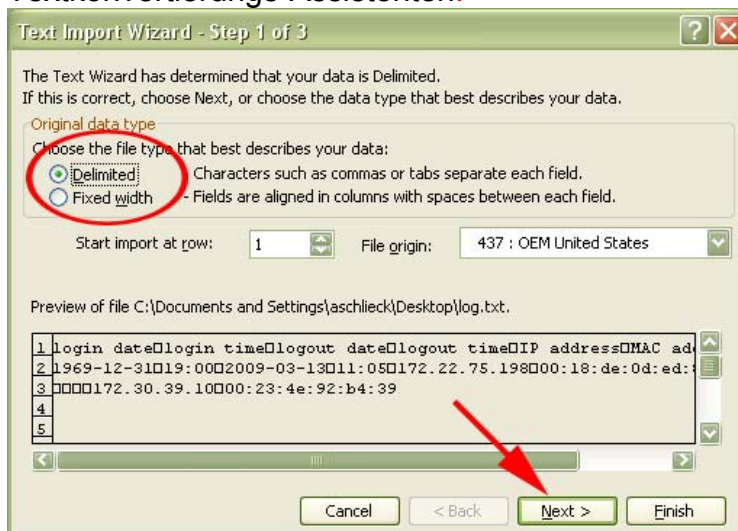


Wählen Sie „Datei speichern“.

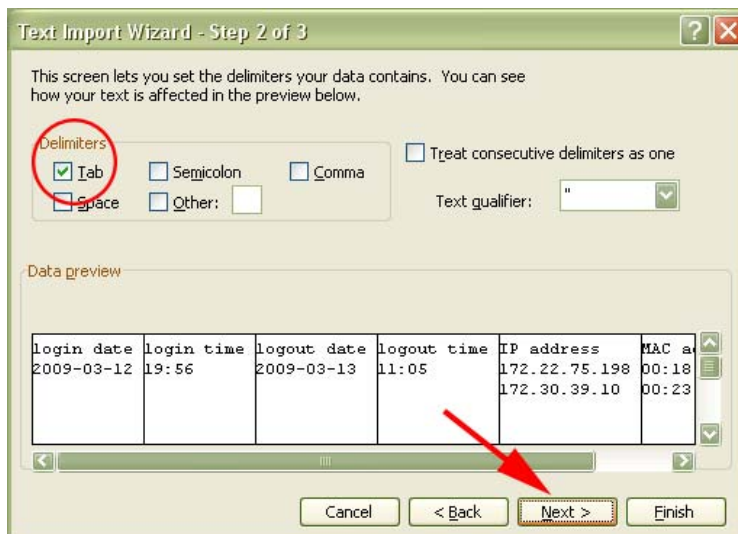


Legen Sie den Zielordner fest, ändern Sie den Dateinamen „config.cgi“ in „log.txt“ um. Klicken Sie auf „Speichern“.

Starten Sie MS Excel und öffnen Sie die Datei log.txt. Sie sehen daraufhin den Textkonvertierungs-Assistenten.

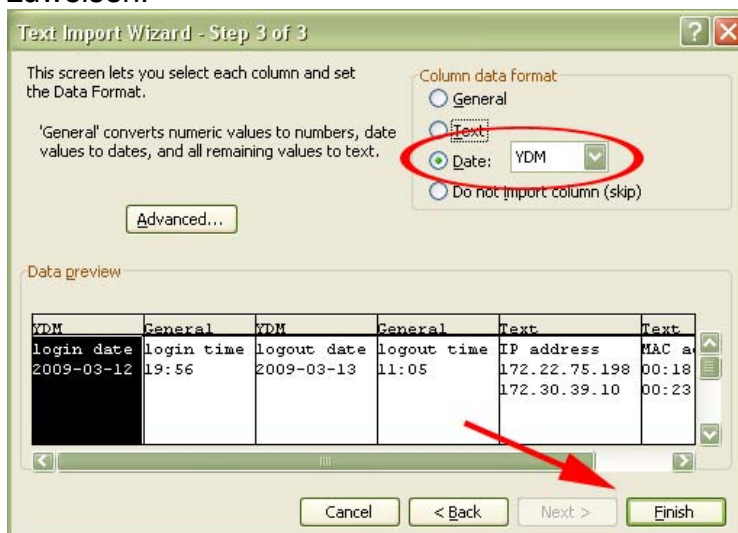


Wählen Sie „Getrennt“ aus und klicken Sie auf „Weiter“.



Wählen Sie „Tabstopp“ aus und klicken Sie auf „Weiter“.

Im nächsten Schritt können Sie den jeweiligen Spalten verschiedene Formate zuweisen.



Empfohlene Werte für die Spalten „login date“ und „logout date“ sind „Datum TMJ“.

Klicken Sie auf „Beenden“, woraufhin MS Excel die Log-Datei öffnet.

### 3. Konfiguration

Sie können ein Backup der Konfiguration erstellen, indem Sie auf „herunterladen“ klicken. Speichern Sie die Datei „config.cgi“ auf Ihrer Festplatte.

Möchten Sie die Konfiguration später wieder nutzen, klicken Sie auf „Browse ...“, wählen Sie die zuvor gespeicherte Datei „config.cgi“ aus und klicken Sie auf „Öffnen“. Zuletzt klicken Sie auf „Laden“, um die Konfigurationsdaten wiederherzustellen.

### 4. Firmware

Bitte lesen Sie hierzu den folgenden Abschnitt „Firmware aktualisieren“.

## **Firmware aktualisieren**

### Wo Sie eine neue Firmware erhalten

Sie können auf zwei Arten herausfinden, ob eine neue Firmwareversion verfügbar ist.

a) Schauen Sie auf die Statusseite von GuestGate

Guest Gate prüft, ob eine neue Firmwareversion verfügbar ist, wenn Sie sich über das Administratormenü einloggen. Wird eine neue Version gefunden, erscheint eine Textnachricht im Statusfenster.

Siehe unteres Beispiel:

### **Gerätestatus-Informationen**

New firmware version available (Version: 1.96 , Date: 2010/07/12 )! [Click here for more information.](#)

Klicken Sie auf den Link "Click here for more information" und Sie werden auf Webseite mit Firmwareinformationen weitergeleitet.

b) Überprüfen Sie den Download-Bereich auf [www.intellinet-network.com](http://www.intellinet-network.com)

### Aktualisierungsvorgang:

Öffnen Sie den Einstellungsbildschirm im Administratormenü.

Klicken Sie auf "Browse" (Durchsuchen), um das neue Firmwarebild auszuwählen, z. B. "524827-2.02.img".

Klicken Sie auf „Installieren“, um den Aktualisierungsvorgang zu starten.

Abhängig von Ihrer Verbindungsgeschwindigkeit zu GuestGate kann die Aktualisierung einige Minuten in Anspruch nehmen.



GuestGate wird nach der Aktualisierung automatisch neu gestartet. Nach der Neustartnachricht müssen Sie 60 Sekunden warten bevor Sie GuestGate nutzen können.

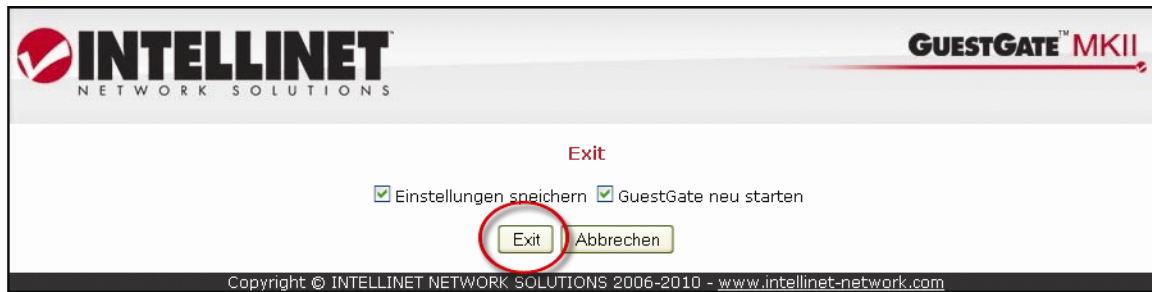
Hinweis:

**Der Aktualisierungsvorgang darf nicht unterbrochen werden!**

Ein Netzwerkverbindungsabbruch oder ein Absturz Ihres lokalen Computers während des Aktualisierungsvorgangs, kann das GuestGate dauerhaft Schaden nehmen.

Idealerweise führen Sie die Aktualisierung innerhalb des lokalen Gastgebernnetzwerks durch, wann immer dies möglich ist. Defekte die durch unsachgemäß durchgeführte Firmwareaktualisierungen verursacht wurden, sind von der Produktgarantie ausgeschlossen.

## Exit-Bildschirm



Mit dieser Seite können Sie die neuen Einstellungen speichern.

### [x] Einstellungen speichern

Alle Änderungen, die Sie an der Konfiguration (den Einstellungen) vornehmen, werden nur übernommen, wenn sie sie über dieses Kästchen speichern.

Haben Sie in irgendeinem Bereich Änderungen vorgenommen und schließen den Browser, ohne diesen letzten Schritt durchgeführt zu haben, gehen alle Änderungen verloren.

### [x] GuestGate neu starten

Um die neuen Einstellungen auch zu aktivieren, müssen Sie hier einen Haken setzen.

#### Hinweis:

Das Speichern der Einstellungen aktiviert diese nicht automatisch, GuestGate muss dazu neu gestartet werden. So können Sie Einstellungsänderungen vornehmen, (z. B. neues Gastpasswort) und erst später aktiv werden lassen.

Nach jedem Neustart von GuestGate, müssen sich alle verbundenen Nutzer erneut authentifizieren.

## FRAGEN & ANTWORTEN

1. **Q:** *Wie lautet die Standard-IP-Adresse des GuestGate?*  
**A:** Die Standard-IP-Adresse lautet: 192.168.2.1
2. **Q:** *Wie lautet das Standard-Administratorpasswort des GuestGate?*  
**A:** Das Standardpasswort lautet: 1234
3. **Q:** *Wie setze ich GuestGate auf die Werkseinstellungen zurück?*  
**A:** Halten Sie die Reset-Taste auf der Rückseite des Geräts 5 Sekunden lang gedrückt, während sich GuestGate im laufenden Betrieb befindet.
4. **Q:** *Ich habe einige Einstellungen im Administrator-Webinterface geändert, aber die Änderungen werden nicht wirksam. Warum?*  
**A:** Eventuell haben Sie vergessen, die Einstellungen auf der EXIT-Seite des Administrator-Webinterfaces zu speichern.
5. **Q:** *Ich habe einen Server in meinem Netzwerk, auf den meine Gäste keinen Zugriff haben sollen. Welche Einstellungen muss ich dafür vornehmen?*  
**A:** Sie müssen keine Einstellungen vornehmen, GuestGate unterstützt diese Funktion standardmäßig. Sollte ein Gast versuchen auf einen Server oder Computer in Ihrem Netzwerk zuzugreifen, wird GuestGate dies unterbinden und im Webbrowser des Gastcomputers einen Warnhinweis anzeigen.
6. **Q:** *Was, wenn ich meinen Gästen Zugriff auf mein Netzwerk, z.B. meinen Intranet-Webserver, gestatten möchte?*  
**A:** Geben Sie die IP-Adresse Ihres Intranet-Servers in den Host-Einstellungen des GuestGates im Menüpunkt „Freigegebene (Erlaubte) Adressen“ an, woraufhin GuestGate den Zugriff auf diesen Server gestattet.
7. **Q:** *Kann ich die Bandbreite der Gastcomputer kontrollieren?*  
**A:** Ja. Upload- und Download-Bandbreiten können in den Gästeeinstellungen des GuestGates im Administratormenü festgelegt werden.
8. **Q:** *Ich möchte die Start/Willkommenseite selbst gestalten. Kann ich die Standard-Seite ändern?*  
**A:** Ja. Die Willkommenseite kann in den entsprechenden Einstellungen des Administratormenüs geändert werden. Sie können den Text ändern und Ihr eigenes Logo/Banner hochladen. Im “erweiterten Modus” haben Sie Zugriff auf den vollständigen HTML-Quellcode, mit dem Sie das Aussehen der Willkommenseite ändern können.

9. **Q:** *Kann ich HTML-Code für meine Willkommenseite nutzen?*  
**A:** Ja. GuestGate schränkt Sie hier in keinsten Weise ein. Sie können den HTML-Code direkt im Konfigurations-Feld der Willkommenseite einfügen. Im „erweiterten Modus“ haben Sie Zugriff auf den vollständigen HTML-Quellcode.
10. **Q:** *Ich habe Änderungen an der Willkommenseite im „erweiterten Modus“ vorgenommen und nun funktioniert sie nicht mehr korrekt. Wie kann ich die Standard-Willkommenseite wiederherstellen?*  
**A:** Öffnen Sie die Einstellungen zur Anpassung der Willkommenseite und stellen Sie sicher, dass der erweiterte Modus aktiv ist. Scrollen Sie nach unten zur „HTML-Code der Willkommenseite“ und klicken Sie auf „Standard-Willkommenseite wiederherstellen“. Speichern Sie über die EXIT-Seite, um diese Einstellung zu aktivieren.
11. **Q:** *Wozu dient die Einstellung „Separates Netzwerk für jeden Benutzer“ in der Gastkonfiguration des GuestGates?*  
**A:** Hierbei handelt es sich um die Layer 3 Client Isolation von GuestGate. Wenn diese Option aktiviert ist, verhindert GuestGate durch Zuweisen von zufälligen, unterschiedlichen TCP/IP-Netzwerkeinstellungen an die angeschlossenen Gastcomputer, dass Gäste sich untereinander „sehen“ können. Auf diese Weise arbeitet jeder Gast in seinem eigenen „Virtual LAN“. Die beiden folgenden Beispiele zeigen die Funktionsweise:
1. Gast-Einstellungen stehen auf „Alle Benutzer operieren im selben Netzwerk (automatisch)“  
Gastcomputer 1 erhält die IP-Adresse 172.16.254.253.  
Gastcomputer 2 erhält die IP Adresse 172.16.254.252.  
Gastcomputer 3 erhält die IP Adresse 172.16.254.251  
[...]  
In diesem Modus arbeiten alle Gastcomputer in einem Netzwerk und können so gegenseitig aufeinander zugreifen. Dies ist der Standard-Modus von nahezu jedem gängigen Router und DHCP-Server auf dem Markt.
2. Gast-Einstellungen stehen auf „separates Netzwerk für jeden Benutzer.“  
Gastcomputer 1 erhält die IP-Adresse 192.168.17.42.  
Gastcomputer 2 erhält die IP Adresse 172.16.25.12.  
Gastcomputer 3 erhält die IP Adresse 10.10.8.178.  
Gastcomputer 4 erhält die IP Adresse 10.10.4.18.  
Gastcomputer 5 erhält die IP Adresse 192.168.8.178.  
[...]  
In diesem Modus arbeitet jeder Gastcomputer in seinem eigenen Netzwerk und hat deshalb keinen Zugriff auf ein anderes Netzwerk mit Ausnahme des Internets. Da diese Funktion mit zufällig generierten Netzwerken arbeitet, ist es für Hacker nahezu unmöglich herauszubekommen, welche IP-Adresse ein anderer Gast hat.
12. **Q:** *Unterstützt GuestGate PHP, ASP oder Perl?*  
**A:** Nein. GuestGate unterstützt keine serverbasierten Scriptsprachen.
13. **Q:** *Wie oft muss ein Gast die Willkommenseite bestätigen?*  
**A:** Nur einmal. Solange der GuestGate nicht neu gestartet wird, wird der Gast kein weiteres mal aufgefordert, das Passwort einzugeben und Ihren Allgemeinen Geschäftsbedingungen zuzustimmen. Hat ein Gast die Verbindung zum GuestGate länger als 10 Minuten unterbrochen, wird die Willkommenseite bei der folgenden Internetverbindung wieder angezeigt.

14. **Q:** *Die Wireless Signalreichweite von GuestGate reicht nicht aus. Wie kann ich die Abdeckung erhöhen?*  
**A:** Sie können zusätzliche WLAN-Access-Points an die LAN-Ports von GuestGate anschließen oder zusätzliche Access Points als Repeater verwenden. Per Kabel angeschlossene, zusätzliche Access Points sind vorzuziehen. Sie bieten ein stabileres WLAN mit höherer Performance und sind einfacher zu konfigurieren.
15. **Q:** *Wie stelle ich WLAN-Sicherheit wie WPA/WPA2-Verschlüsselung ein?*  
**A:** Die WLAN-Funktionen von GuestGate unterstützen keine Verschlüsselung. Sie können den Internetzugang über die diversen Gastpassworteinstellungen sichern. Benötigen Sie ein verschlüsseltes Wireless Netzwerk, müssen Sie externe Access Points mit GuestGate verbinden und die interne WLAN-Funktion deaktivieren.
16. **Q:** *Kann ich über einen der Gast-Ports auf das Administratormenü zugreifen?*  
**A:** Nein. Aus Sicherheitsgründen ist dies nicht möglich. Zugriff auf das Administratormenü kann nur über den Host-Port erfolgen.
17. **Q:** *Kann ich über das Gastgeber Netzwerk auf einen der Gastcomputer zugreifen?*  
**A:** Nein. Ports zu öffnen, um Computer zu verbinden (gängig bei Standard-Routern - Virtual Server/Port-Weiterleitung), ist bei GuestGate aus Sicherheitsgründen nicht möglich.
18. **Q:** *Kann ich in GuestGate Ports öffnen, um direkten Zugang auf einen verbundenen Gastcomputer zu erhalten?*  
**A:** Nein, dies ist nicht möglich. Siehe Frage 17.
19. **Q:** *Einige meiner Gäste möchten ein Netzwerkspiel spielen oder Dateien und Verzeichnisse freigeben, was leider nicht funktioniert. Wie kommt es, dass die angeschlossenen Gastcomputer nicht untereinander kommunizieren können?*  
**A:** Das liegt daran, dass standardmäßig Layer 3 Client aktiviert ist. Sie müssen dies zunächst deaktivieren, um eine Kommunikation zwischen den angeschlossenen Gastcomputern zu ermöglichen. (Siehe dazu Frage 11)
20. **Q:** *Auf der Status-Seite des Web-Administrationsinterface wird die Zeit als "(nicht verfügbar)" angezeigt, wieso?*  
**A:** GuestGate kann auf die Pool Time Server des Internets nicht zugreifen und kann daher keine gültige Systemzeit abfragen. Das liegt wahrscheinlich daran, dass eine Firewall im Gastgeber Netzwerk ausgehende Network Time Protocol (NTP) Anfragen blockiert. Der Systemadministrator muss die benötigten Ports öffnen (Port 123 für TCP und UDP). Dies ist besonders wichtig, wenn Sie die "Zeit / Planer"-Funktion nutzen möchten.



21. **Q:** *Regelt die Bandbreitenbegrenzung die Bandbreite pro Computer oder die Bandbreite, die das GuestGate insgesamt zur Verfügung stellt?*

**A:** Die Bandbreitenbegrenzung reguliert die Bandbreite, die das GuestGate nutzen kann, egal wie viele Gäste sich mit dem Gerät verbunden haben.

## ANHANG

Im Folgenden finden Sie eine Liste aller gängigen TCP/IP Service-Ports. Diese Ports können in der Gastgeber-Konfiguration von GuestGate eingegeben werden, um den Zugriff auf bestimmte Dienste zu verweigern.

Port-Nummer	Service-Name / Beschreibung
21	FTP
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Ausgehende Mails, Sendmail Server Port)
69	TFTP (Trivial File Transfer Protocol)
70	Gopher
79	Finger
80	HTTP (Standard- Webport für Webseiten)
110	POP3 (Eingehende Mails)
115	SFTP (Simple File Transfer Protocol)
119	NNTP (Newsgroups)
123	NTP (Network Time Protocol)
135	RPC Service, verwendet für NET SEND Befehl
137, 138, 139	NETBIOS (Filesharing, MS Windows Network)
143	IMAP (Interim Mail Access Protocol)
161	SNMP (Simple Network Management Protocol)
194, 6665-6669	IRC (Internet Relay Chat)
443	HTTPS (Secure Web transfer, verwendet von SSL))
514	SHELL
515	LPR (Line Printer Remote), LPD (Line Printer Daemon)
631	IPP (Internet Printing Protocol)
1080, 3127, 3128, 10080	<u>Trojan</u> : verwendet von MyDoom
1723	PPTP (verwendet für VPN-Verbindungen)
1863	MSN Messenger
2535, 2745, 8866	<u>Trojaner</u> : Verwendet von Beagle
3389	Windows XP Remote Desktop Port
3410	<u>Trojan</u> : OptixPro, also used by NetworkLens SSL Event
3689	iTUNES von Apple, DAAP
4899	RADMIN, Fernzugriff
5000, 5001	YAHOO Messenger Voice Chat
5100	YAHOO Messenger Video (Webcam)
5190, 5191, 5192, 5193	AOL (America On Line via TCP)
5554	Trojaner: Sasser-Familie, auch verwendet für SGI ESP HTTP.
5800+, 5900+	VNC
12345	<u>Trojaner</u> : Verwendet von Netbus, außerdem von Italk Chat System und TrendMicro OfficeScan Antivirus
27374	<u>Trojaner</u> : Verwendet von SubSeven

# GARANTIEINFORMATIONEN

<b>Deutsch</b>	Garantieinformationen finden Sie unter <a href="http://www.intellinet-network.com/warranty">www.intellinet-network.com/warranty</a> .
<b>English</b>	For warranty information, go to <a href="http://www.intellinet-network.com/warranty">www.intellinet-network.com/warranty</a> .
<b>Español</b>	Si desea obtener informaci3n, visite <a href="http://www.intellinet-network.com">www.intellinet-network.com</a> .
<b>Français</b>	Pour consulter les informations, allez sur <a href="http://www.intellinet-network.com">www.intellinet-network.com</a> .
<b>Italiano</b>	Per informazioni sulla garanzia, visitate <a href="http://www.intellinet-network.com">www.intellinet-network.com</a> .
<b>Polski</b>	Informacje dotyczące gwarancji znajdują się na stronie <a href="http://www.intellinet-network.com/warranty">www.intellinet-network.com/warranty</a> .
<b>México</b>	Poliza de Garantía INTELLINET — Datos del importador y responsable ante el consumidor IC Intracom México, S.A. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlán Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500

La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra.

A. Garantizamos cámaras IP y productos con partes móviles por 3 años.

B. Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones:

1. Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor.
2. El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico.
3. La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instalados en fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor.

Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde fue adquirido o en el domicilio de IC Intracom México, S.A. de C.V., junto con los accesorios contenidos en su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora (indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, número de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese utilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; ó si el producto ha sido alterado o tratado de ser reparado por el consumidor ó terceras personas.



INTELLINET NETWORK SOLUTIONS™ bietet ein vollständiges Sortiment  
aktiver und passiver Netzwerkkomponenten.  
Für weitere Informationen wenden Sie sich bitte an Ihren Händler oder nutzen Sie die Webseite

**[www.intellinet-network.com](http://www.intellinet-network.com)**

Copyright © INTELLINET NETWORK SOLUTIONS  
Alle genannten Produkte sind eingetragene Marken oder Marken der jeweiligen Firmen.